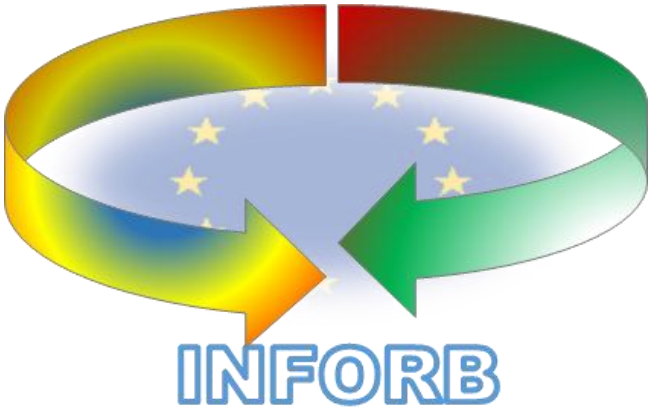

STUDIU ȘI MANUAL PRIVIND SECURITATEA CIBERNETICĂ ȘI LANȚUL DE APROVIZIONARE PENTRU SECTORUL ALIMENTAR

LIVRABIL D4.1

Versiunea V1.0

REZUMAT

Acest document este structurat în două părți, având ca scop consolidarea securității cibernetice în sectorul alimentar din România și Bulgaria, în conformitate cu Directiva NIS2 și creșterea digitalizării.

Titlul I – **Studiu privind securitatea cibernetică în sectorul alimentar** evaluează nivelul de maturitate al securității cibernetice, evidențiind tendințele de digitalizare, vulnerabilitățile IMM-urilor, principalele amenințări cibernetice și alinierea la standardele UE. Pe baza sondajelor, a rapoartelor ENISA și a datelor din sursă deschisă, acesta oferă concluzii și recomandări specifice pentru a spori reziliența cibernetică.

Titlul II – **Manualul de gestionare a riscurilor de securitate cibernetică în lanțul de aprovizionare** oferă un cadru practic pentru identificarea și atenuarea riscurilor cibernetice de-a lungul lanțului de aprovizionare digital. Încorporează standarde internaționale (ISO/IEC 27005, NIST RMF) și cadre legale naționale, punând accentul pe garanțiile tehnice, responsabilitățile organizaționale și conformitatea cu reglementările.

Împreună, aceste componente formează un instrument valoros pentru organizațiile din sectorul alimentar care doresc să îmbunătățească postura de securitate cibernetică, să asigure conformitatea și să promoveze reziliența operațională.

Informații despre controlul documentelor

Setări	Valoare
Titlul documentului:	Studiu și manual privind securitatea cibernetică și lanțul de aprovizionare pentru sectorul alimentar
Numărul proiectului:	101128047
Nume proiect:	Implementarea Directivei NIS în sectorul producției, procesării și distribuției de alimente din România și Bulgaria
Acronimul proiectului:	INFORB
Autorul (autorii) documentului:	Gheorghiță Comăneci, Silviu-Nicolae Dorobanțu, Rozalia Parapuf, Diana Opriș, Gergana Rakova, Eli Kuyamova, Panayotka Panayotova
Identificator livrabil:	D4.1
Termen de livrare:	30.06.2025
Data livrării:	24.06.2025
Manager de proiect (PM):	Constantin Călin
Versiunea documentului:	V1.0
Sensibilitate:	PU-Public
Dată:	23.06.2025

Evaluarea documentelor și evaluatorii

Nume	Rol	Acțiune	Dată
Gheorghiță Comăneci	Coordonator WP4	Proiect de document creat	22.11.2024
Silviu Dorobanțu	Expert în securitate cibernetică	Versiunea originală (DNSC)	20.05.2025
Gergana Rakova	Proiect	Actualizare versiune (MGBEG)	20.06.2025
Eli Kuyamova	Expert IT de proiect		
Panayotka Panayotova	Lider de proiect al echipei BG		
Consiliul consultativ de experți	Evaluare	Versiune convenită	23.06.2025
Constantin Călin	Manager de proiect	Documentul final preluat și livrat	24.06.2025

Istoricul documentului

Recenzie	Dată	Creat de	Scurtă descriere a modificărilor
V0	12.12.2024	Expert în securitate cibernetică	Proiect de document creat. Documentare, analiza surselor. Documentare, analiza surselor.
V0.1	16.04.2025	Expert în securitate cibernetică și Coordonator WP4	Rectificarea documentului actualizat cu informații

V0.1.1	23.04.2025	Expert în securitate cibernetică	Document actualizat
V0.1.2	08.05.2025	Expert în securitate cibernetică	Actualizați cu informații
V0.2	20.05.2025	Expert în securitate cibernetică	Actualizarea documentului (limba română)
V0.3	23.05.2025	Expert în securitate cibernetică	Tradus în engleză
V0.4	20.06.2025	Coordonator/Lider de proiect	Actualizat de experți bulgari
V1.0	23.06.2025	Coordonator WP4 și expert în securitate cibernetică	Documentul final versiunea 1

Cuprins

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

TITLUL 1. STUDIU PRIVIND SECURITATEA CIBERNETICĂ ÎN SECTORUL ALIMENTAR

Abstract

Această parte evaluează maturitatea în materie de securitate cibernetică a sectorului alimentar din România și Bulgaria, cu accent tehnic pe nivelurile de digitalizare, vulnerabilitățile specifice ale întreprinderilor mici și mijlocii (IMM-uri), principalele amenințări cibernetice și gradul de conformitate cu standardele UE de securitate cibernetică. Bazându-se pe sondaje structurate, evaluări ale amenințărilor ENISA și date din surse deschise, studiul identifică lacune în controalele tehnice, cum ar fi segmentarea insuficientă a rețelei, lipsa protecției endpoint-urilor și capacitățile limitate de răspuns la incidente. Constatările sunt utilizate pentru a dezvolta recomandări specifice menite să sporească reziliența cibernetică în întregul sector, inclusiv adoptarea unor cadre de securitate standardizate, clasificarea activelor bazate pe risc și monitorizarea îmbunătățită a infrastructurii digitale critice.

SECȚIUNEA 1. INTRODUCERE

Sectorul alimentar trece printr-un proces accelerat de digitalizare, integrând tehnologii IT și sisteme automatizate în producția, procesarea, depozitarea și distribuția alimentelor. Această transformare digitală aduce multiple beneficii în ceea ce privește eficiența și trasabilitatea, dar deschide și noi vulnerabilități în fața amenințărilor cibernetice.

În ultimii ani, au fost raportate incidente semnificative care demonstrează impactul real al atacurilor cibernetice asupra lanțului alimentar: de exemplu, în aprilie 2021, un atac ransomware a vizat un distribuitor olandez de alimente, blocând comunicarea dintre depozite și clienți și lăsând rafturile unui mare lanț de supermarketuri fără produse timp de câteva zile. La scurt timp după aceea, cel mai mare procesator de carne din lume a fost forțat să-și închidă temporar operațiunile din SUA, Canada și Australia în urma unui alt atac ransomware. Astfel de incidente evidențiază nevoia urgentă de a consolida securitatea cibernetică în sectorul alimentar.

Securitatea cibernetică în acest domeniu nu înseamnă doar protejarea datelor companiei, ci și asigurarea continuității producției și distribuției alimentelor – un element esențial al securității alimentare naționale și chiar globale. Sectorul alimentar este considerat parte a infrastructurii critice, deoarece compromiterea sa poate avea consecințe grave asupra populației (de la penurie de alimente la riscuri pentru sănătate). Cu toate acestea, din punct de vedere istoric, acest sector nu a primit același nivel de atenție în politicile de securitate cibernetică ca alte sectoare (cum ar fi finanțele sau energia). De aceea, acest studiu își propune să evalueze starea actuală a securității cibernetice în industria alimentară, identificând principalele riscuri, provocări și măsuri specifice de protecție, pe baza datelor colectate de la organizațiile din domeniu și a ghidurilor furnizate de organisme specializate la nivel european.

În continuare, vom prezenta obiectivele și metodologia studiului, analiza detaliată a datelor unui sondaj realizat în rândul companiilor din sectorul alimentar din România și Bulgaria, vom integra perspectivele actuale din publicațiile ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) privind securitatea cibernetică în sectorul alimentar sau în sectoarele conexe și vom formula concluzii și recomandări menite să sprijine îmbunătățirea nivelului de securitate cibernetică în acest sector critic.

Obiectivele studiului

Evaluarea nivelului de maturitate digitală și a practicilor de securitate cibernetică în companiile alimentare – prin analiza caracteristicilor organizațiilor (dimensiune, locație, profil de activitate) și a

infrastructurii IT&C utilizate, inclusiv modul în care acestea implementează sau externalizează serviciile de securitate cibernetică.

Identificarea principalelor riscuri și amenințări cibernetice percepute în sectorul alimentar – pe baza datelor sondajelor și a analizelor calitative (inclusiv răspunsuri deschise la probleme de securitate), precum și evidențierea diferențelor pe baza unor factori precum dimensiunea organizației sau regiunea geografică.

Compararea situației din sectorul alimentar cu tendințele și cele mai bune practici la nivel european, din perspectiva ENISA – inclusiv statistici recente privind incidentele cibernetice din sectorul alimentar, prevederi de reglementare (de exemplu, extinderea domeniului de aplicare al Directivei NIS2) și prognoze privind evoluția amenințărilor cibernetice în acest domeniu.

Formularea de concluzii și recomandări specifice pentru îmbunătățirea securității cibernetice în sectorul alimentar – adresate atât organizațiilor din industrie (producători, procesatori, distribuitori etc.), cât și factorilor de decizie sau partenerilor tehnologici, pentru a reduce vulnerabilitățile și a crește reziliența cibernetică a lanțului alimentar.

Metodologii

- **Colectarea datelor sondajului**

Un chestionar a fost realizat folosind platforma EU Survey, în numele celor două județe separat (în versiunea BG, EN și RO). Aceste chestionare au fost destinate organizațiilor din sectorul alimentar din România și Bulgaria, acoperind subiecte precum profilul companiei, infrastructura IT și practicile de securitate cibernetică. Sondajul a inclus atât întrebări închise (pentru a cuantifica utilizarea anumitor tehnologii sau servicii), cât și întrebări deschise (pentru a identifica percepțiile cu privire la riscurile cibernetice și provocările întâmpinate). Au răspuns în total 62 de organizații din România în domeniu. Până la 19.06.2025, în Bulgaria au răspuns la sondaj 38 de entități. Sondajul BG rămâne deschis pentru răspunsuri suplimentare. Răspunsurile sunt anonimizate și agregate pentru analiză.

- **Analiza datelor**

Datele colectate au fost analizate statistic (analiză descriptivă și corelativă). A fost examinată distribuția respondenților în funcție de diferite criterii (tip de organizație, dimensiune, regiune, subsector alimentar), a fost evaluat gradul de adoptare a soluțiilor de securitate cibernetică (intern vs. externalizare) și au fost identificate tendințe sau corelații semnificative (de exemplu, în funcție de dimensiunea organizației sau regiunea geografică). De asemenea, a fost aplicată o analiză de segmentare (clustering) a organizațiilor în funcție de practicile IT&C și de securitate, pentru a evidenția posibile **profiluri distincte de maturitate cibernetică**.

- **Analiză calitativă**

Răspunsurile la întrebările deschise din sondaj au fost analizate pentru a extrage principalele **teme și preocupări legate de riscurile cibernetice**. De asemenea, a fost creat un nor de cuvinte de termeni menționați frecvent, pentru a identifica rapid riscurile percepute ca fiind cele mai importante. Această analiză textuală a oferit o imagine de ansamblu a conștientizării amenințărilor în rândul organizațiilor.

- **Documentarea și integrarea surselor ENISA**

Pentru a corela rezultatele sondajului cu contextul european, au fost consultate publicații recente ale ENISA și ale altor organisme relevante. Au fost analizate rapoarte privind peisajul amenințărilor, ghiduri de bune practici și dispoziții de reglementare (cum ar fi Directiva NIS2) aplicabile sectorului alimentar sau sectoarelor conexe (agroalimentar, lanț de aprovizionare, IMM-uri). Informațiile relevante din aceste surse au fost integrate într-un capitol separat al studiului, pentru a evidenția **alinierea situației din România la tendințele și recomandările UE**.

- **Delimitarea și structurarea relației**

Conținutul studiului a fost organizat în secțiuni clare (introducere, metodologie, analiză, concluzii etc.) în funcție de cerințele unui raport de cercetare. Graficele și tabelele rezultate din analiză au fost incluse pentru a susține vizual concluziile, fiecare figură fiind însoțită de un titlu și explicații relevante. La final, este furnizată o bibliografie care enumeră sursele consultate și citate în document.

SECȚIUNEA 2. REZULTATELE ANALIZEI DATELOR SONDAJULUI

Profilul organizațiilor respondente

Sondajul a implicat 62 de organizații din sectorul alimentar din România și până la 19.06.2025 – 38 de organizații din sectorul alimentar din Bulgaria, acoperind diferite verigi din lanțul de aprovizionare cu alimente. **Tipul de organizație** indică o predominanță a companiilor private – toate entitățile respondente fiind firme private. Acest lucru poate fi explicat prin structura economică a sectorului, în care inițiativa privată este predominantă. Deși organizațiile de stat sau ONG-urile (de exemplu, autoritățile sanitare, asociațiile producătorilor) sunt, de asemenea, active în industrie, acestea sunt slab reprezentate în eșantionul sondajului, sugerând necesitatea de a înțelege mai bine nevoile lor specifice în viitor.

Situația din România

Din perspectiva **subsectorului alimentar** în care își desfășoară activitatea, respondenții acoperă o gamă largă de activități. Majoritatea (aproximativ 92%) au **operațiuni de producție alimentară** (de la prelucrarea materiilor prime până la fabricarea produselor finite), multe dintre aceste companii au și funcții **integrate de distribuție** (61%) sau **depozitare** (52%) în lanțul logistic. Aproximativ 45% dintre respondenți sunt, de asemenea, implicați în **prelucrarea** (prelucrarea intermediară a produselor alimentare). Aceste procente cumulate depășesc 100%, deoarece multe companii au un model de afaceri integrat (de exemplu, produc alimente și au propriile depozite și rețele de distribuție). Astfel, **eșantionul reflectă o imagine complexă a lanțului agroalimentar**, incluzând atât producătorii primari, cât și unitățile de prelucrare sau distribuitorii angro. Această diversitate ne permite să surprindem provocările de securitate cibernetică de-a lungul lanțului alimentar.

Din punct de vedere geografic, organizațiile sunt răspândite în mai multe regiuni de dezvoltare ale țării, dar nu în mod egal. Există o concentrație semnificativă de respondenți în **regiunea Centru** (care include județe cu tradiție industrial-agrară, de exemplu Mureș, Sibiu, Brașov), urmate de **Bucuresti-Ilfov**, care, în calitate de regiune capitală, acționează ca un pol economic și tehnologic. Cel **Nord-Vest** (de exemplu, Cluj, Bihor) și **Sud-Est** (de exemplu, Constanța, Galați) au și ele o prezență notabilă, în timp ce **Sud** și **Nord-Est** zonele sunt reprezentate mai modest și **Sud-Vest (Oltenia) abia se înscrie în eșantion. Această distribuție reflectă parțial disparitățile economice regionale: regiunile mai dezvoltate economic, cu o infrastructură IT mai solidă (cum ar fi Centru, București-Ilfov, Nord-Vest) au fost mai bine reprezentate, în timp ce cele cu o dezvoltare mai mică apar cu ponderi mici. Figura 1 ilustrează distribuția respondenților pe regiuni de dezvoltare, evidențiind predominanța regiunilor Centru și București-Ilfov față de altele.**

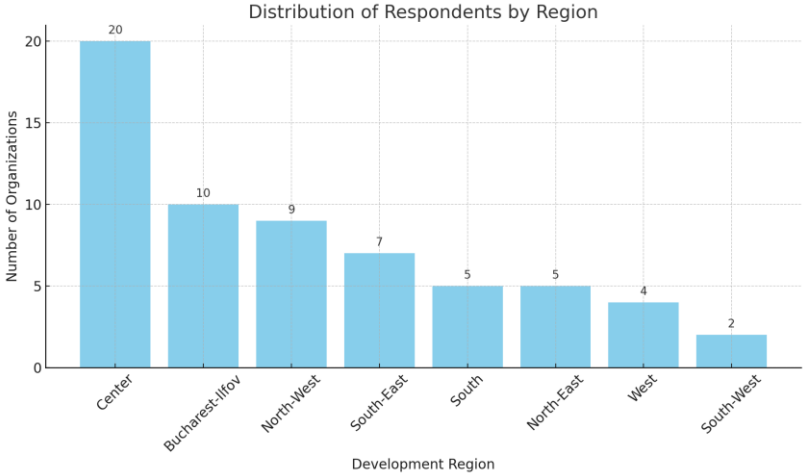

Figura 1. România - Distribuția respondenților pe regiuni de dezvoltare.

Regiunile Centru și București-Ilfov reprezintă aproape jumătate din eșantion, indicând o concentrare a companiilor participante în zonele mai dezvoltate din punct de vedere economic. În schimb, regiuni precum Sud-Vest sau Nord-Est au un număr mult mai mic de organizații respondente, ceea ce poate sugera atât un număr mai mic de companii alimentare cu profil digital în aceste domenii, cât și posibile lacune în gradul de digitalizare și conștientizare a problemelor de securitate cibernetică.

În termeni **de dimensiunea companiei**, predomină întreprinderile mici și mijlocii (IMM-uri). Aproximativ jumătate dintre respondenți se clasifică ca fiind **întreprinderi mijlocii** și o proporție semnificativă a **întreprinderi mari**. Doar foarte puține (cazuri izolate din eșantion) sunt microîntreprinderi sau întreprinderi mici. Acest lucru este în concordanță cu structura generală a economiei naționale, în care IMM-urile formează coloana vertebrală a industriei alimentare, în timp ce întreprinderile mari (deși mult mai puține ca număr) au un impact economic și logistic disproporționat de mare. Relevanța acestei structuri pentru securitatea cibernetică este majoră: IMM-urile au de obicei resurse financiare și umane limitate pentru investiții în securitate, în comparație cu marile corporații care își pot permite echipe dedicate și tehnologii avansate. Astfel, sprijinirea IMM-

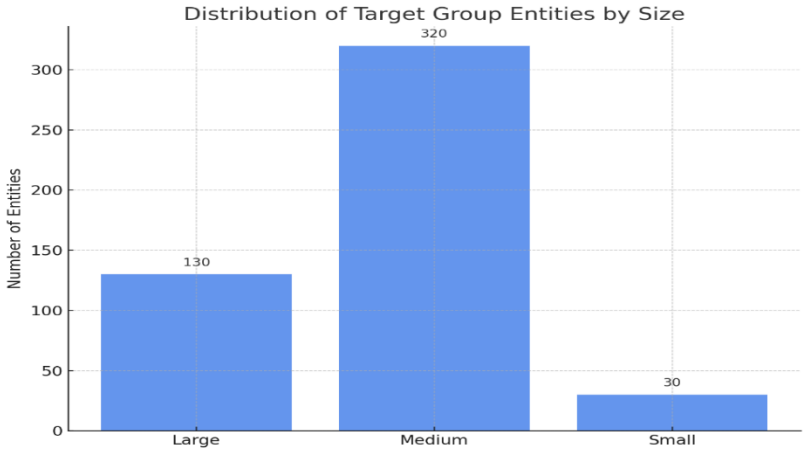

Figura 2. România - Distribuția respondenților în funcție de dimensiunea companiei.

urilor în adoptarea soluțiilor de securitate devine esențială pentru creșterea nivelului general de protecție în sector.

Situația din Bulgaria

Din perspectiva **subsectorului alimentar** în care își desfășoară activitatea, respondenții acoperă o gamă largă de activități. Majoritatea (aproximativ 87%) au **operațiuni de producție alimentară** (de la prelucrarea materiilor prime până la fabricarea produselor finite), unele dintre aceste companii au și **funcții de distribuție** integrată (13%) în lanțul logistic. Aproximativ 18% dintre respondenți sunt, de asemenea, implicați în **prelucrarea** (prelucrarea intermediară a produselor alimentare). Aceste procente cumulate depășesc 100%, deoarece multe companii au un model de afaceri integrat (de exemplu, produc alimente și au propriile depozite și rețele de distribuție). Astfel, **eșantionul reflectă o imagine complexă a lanțului agroalimentar**, incluzând atât producătorii primari, cât și unitățile de prelucrare sau distribuitorii angro. Această diversitate ne permite să surprindem provocările de securitate cibernetică de-a lungul lanțului alimentar.

Din punct de vedere geografic, organizațiile sunt răspândite în mai multe regiuni de dezvoltare ale țării. Există o concentrație semnificativă de respondenți în **regiunea de nord-est** (care include regiuni cu tradiție industrial-agrară (de exemplu, Varna, Dobrich), urmată de **regiunea central-nord.** Regiunile Centru-Sud, **Nord-Vest** și **Sud-Vest** (de exemplu, Sofia) au, de asemenea, o prezență notabilă, în timp ce **zona de Sud-Est (Burgas)** sunt reprezentate mai modest. **Această distribuție reflectă parțial disparitățile economice regionale: regiunile mai dezvoltate din punct de vedere economic cu o infrastructură IT mai solidă (cum ar fi Sofia, Varna) au fost mai bine**

reprezentate, în timp ce cele cu o dezvoltare mai mică apar cu ponderi mici. Figura 1 ilustrează distribuția respondenților pe regiuni de dezvoltare, evidențiind predominanța regiunilor de nord-est și nord-centru în comparație cu altele.

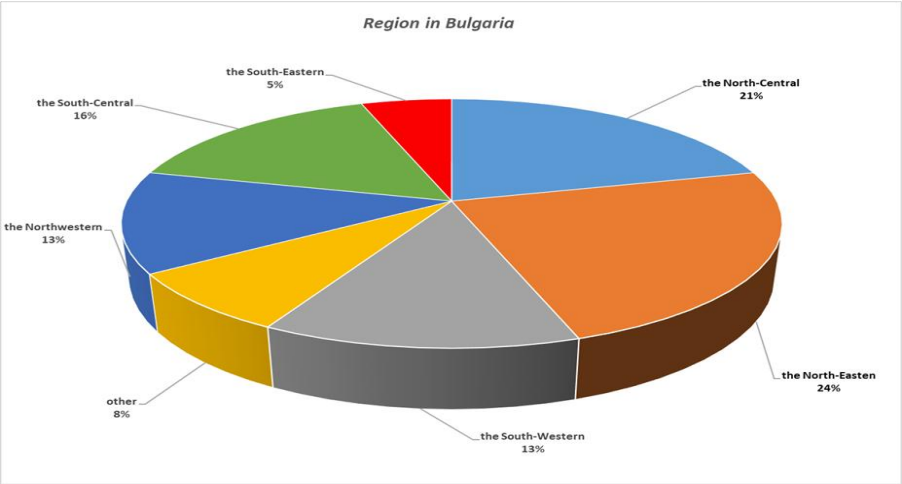

Figura 3. Bulgaria - Distribuția respondenților pe regiuni de dezvoltare.

În termeni **de dimensiunea companiei**, predomină microîntreprinderile sau întreprinderile mici. Doar câteva sunt de dimensiuni medii și mari. Acest lucru este în concordanță cu structura generală a economiei naționale, în care IMM-urile formează coloana vertebrală a industriei alimentare. IMM-urile au de obicei resurse financiare și umane limitate pentru investiții în securitate, în comparație cu marile corporații care își pot permite echipe dedicate și tehnologii avansate. Astfel, sprijinirea IMM-urilor în adoptarea soluțiilor de securitate devine esențială pentru creșterea nivelului general de protecție în sector. **Figura 3 ilustrează distribuția respondenților în funcție de dimensiunea companiei.**

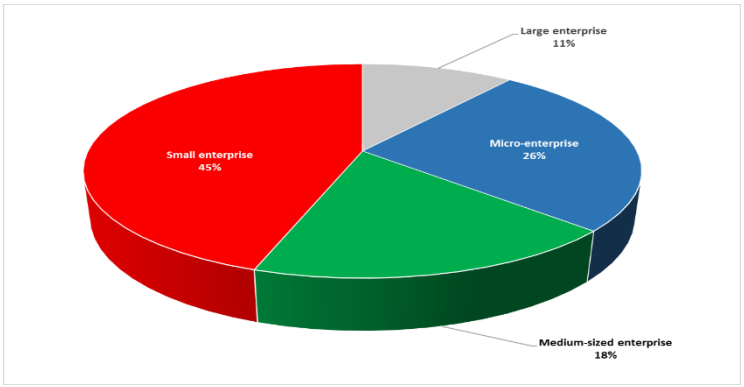

Figura 4. Bulgaria - Distribuția respondenților în funcție de dimensiunea întreprinderii.

Servicii IT și practici de securitate cibernetică

Analiza utilizării **serviciilor IT&C de** către organizațiile din eșantion oferă indicii despre maturitatea lor tehnologică și gradul de preocupare pentru securitate. Serviciile de bază, cum ar fi **întreținerea** sistemului, **administrarea rețelei** și **asistența tehnică**, par a fi cele mai frecvent utilizate – ceea ce este de așteptat, deoarece sunt esențiale pentru funcționarea zilnică a oricărei organizații moderne. De asemenea, multe companii indică utilizarea serviciilor legate de prezența online, cum ar fi

gestionarea unui **site web** sau **a serviciilor de e-mail**. Aceste elemente constituie nivelul fundamental al digitalizării, asigurând operabilitatea și comunicarea continuă a companiei.

Pe de altă parte, **serviciile IT avansate** – de exemplu, soluțiile de cloud computing, automatizarea proceselor industriale, business intelligence – sunt mai degrabă prerogativa organizațiilor mari sau a celor din sectoare percepute ca fiind critice din punct de vedere tehnologic (cum ar fi transportul sau finanțele). Doar o fracțiune dintre companiile alimentare care au răspuns (cele cu resurse mai substanțiale) au menționat utilizarea unor astfel de soluții avansate, ceea ce indică un **grad inegal de digitalizare** în cadrul sectorului: câteva firme de vârf de lance care adoptă tehnologii de ultimă oră, în timp ce majoritatea rămân la nivelul instrumentelor de bază necesare pentru a funcționa.

În special în ceea ce privește **soluțiile și măsurile de securitate cibernetică adoptate**, am găsit variații semnificative între organizații. Un aspect central este modul **de gestionare a funcției de securitate cibernetică**: internă (cu personal propriu și resurse locale) sau externalizată (prin contractarea furnizorilor specializați). Rezultatele pentru România arată că există patru situații majore (vezi Figura 4):

- Organizațiile care **nu au o funcție dedicată securității cibernetice** (fie nu consideră aplicabile, fie nu au servicii specializate) – aproximativ o treime din eșantion (34%) se află în această situație, ceea ce poate indica un risc latent, aceste companii mizând probabil doar pe măsurile minime implementate de echipele IT generale.
- Organizații care gestionează **securitatea exclusiv intern** – în ~34% din cazuri, companiile se bazează pe propriul personal IT pentru a asigura securitatea (instalare de antiviruși, firewall, întreținere de securitate etc.), fără a recurge la servicii externe.
- Organizațiile care **externalizează integral** serviciile de securitate cibernetică – reprezentând aproximativ 11% dintre respondenți, au contracte cu furnizori specializați (MSP/MSSP) care se ocupă de protecția infrastructurii lor.
- Organizații care au o abordare hibridă **(mix intern și externalizat)** – aproximativ 21% dintre respondenți folosesc o combinație: păstrează unele sarcini de securitate intern, dar externalizează anumite servicii critice (de exemplu, monitorizare 24/7, audit de vulnerabilitate sau răspuns la incidente).

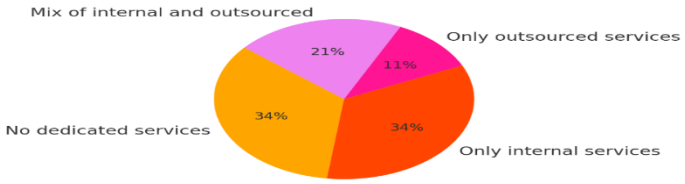

Figura 5. România - Cum sunt gestionate serviciile de securitate cibernetică în companiile respondente.

Se poate observa că doar o mică parte (aproximativ 11%) se bazează exclusiv pe servicii externalizate, în timp ce majoritatea preferă fie soluții interne (personal propriu), fie o combinație a celor două. În special, o treime dintre companii nu au servicii de securitate dedicate, ceea ce indică o potențială vulnerabilitate – fie aceste companii sunt foarte mici și nu au considerat necesar, fie există o lipsă de conștientizare a riscurilor cibernetice. În același timp, procentul ridicat al celor care folosesc **doar soluții interne** reflectă preferința IMM-urilor pentru opțiuni cu costuri reduse și control local, dar aceste soluții interne sunt adesea **soluții de bază** (de exemplu, antivirus gratuit, firewall implicit) care pot fi insuficiente împotriva amenințărilor avansate.

În ceea ce privește **tehnologiile de securitate implementate**, datele arată că **măsurile de bază sunt relativ bine reprezentate**:

- Aproape toate organizațiile au raportat că folosesc un **antivirus** pe stațiile lor de lucru – de fapt, 98% au confirmat că toate computerele și laptopurile lor sunt protejate cu soluții antivirus actualizate. Acest lucru arată că nivelul minim de protecție a endpoint-urilor este asigurat în majoritatea cazurilor.
- În ceea ce privește **firewall-urile** de rețea (sau soluțiile Next-Generation Firewall), ~84% dintre organizații au o astfel de soluție (fie sub formă de hardware dedicat, fie ca dispozitiv virtual sau serviciu cloud). Doar 16% au indicat că nu au deloc un firewall, în special entități foarte mici sau probabil în stadiile incipiente de informatizare.
- **Backup-urile** sunt, de asemenea, o practică aproape universală: 92% dintre companii au implementat o soluție de backup regulată pentru date importante, fie local, fie în cloud, asigurându-se astfel că își pot recupera datele în caz de incidente (defecțiuni sau atacuri ransomware).
- Alte soluții de securitate menționate: **sisteme de control acces** (inclusiv controlul domeniului/Active Directory în cazul companiilor mai mari), soluții de securitate a e-mailului (de exemplu, filtre anti-spam, gateway securizat de e-mail), instrumente IDS/IPS pentru detectarea intruziunilor în rețea și, într-o măsură mai mică, soluții de prevenire a pierderii datelor (DLP) sau **WAF (Web Application Firewall)** pentru protecția aplicațiilor web publice.

Cu toate acestea, adoptarea acestor tehnologii de securitate mai avansate (IDS/IPS, DLP, WAF etc.) este **inegală**: companiile mari și cele cu un profil tehnologic mai complex tind să le implementeze, în timp ce IMM-urile tradiționale din industria alimentară sunt de obicei limitate la antivirus, firewall și backup. Principalul motiv invocat în discuțiile informale este legat de **costuri și expertiza necesară** – multe companii mici consideră că setul minim de măsuri este suficient și nu au personal sau buget pentru soluții de întreprindere. Acest lucru evidențiază o potențială **expunere la amenințări avansate** a unei părți semnificative a sectorului: actorii rău intenționați pot exploata lipsa de protecții avansate în IMM-uri pentru a lansa atacuri mai sofisticate (cum ar fi pătrunderea în rețea și mișcarea laterală nedetectată în absența unui IDS sau exfiltrarea datelor sensibile dacă nu există DLP).

Pe de altă parte, externalizarea securității către firme specializate oferă acces la expertiză și tehnologii de ultimă oră (monitorizare 24/7, threat intelligence, intervenție rapidă), dar nu este lipsită de provocări. Respondenții care au optat pentru externalizare menționează beneficii precum audituri periodice de vulnerabilitate și consultanță strategică, dar recunosc și **riscurile asociate**: blocare, posibile întârzieri în răspuns din cauza contractelor la nivel de servicii, precum și costuri pe termen lung care pot deveni substanțiale. Soluția spre care converg concluziile noastre este cea mixtă: **o combinație strategică de soluții interne și externe** pare a fi abordarea optimă, permițând organizației să mențină controlul asupra problemelor critice și, în același timp, să beneficieze de contribuția expertizei externe acolo unde este necesar.

Analiza relațională a datelor a evidențiat câteva **corelații importante**:

- **Dimensiunea organizației vs. complexitatea tehnologică: Există** o tendință clară ca **organizațiile mai mari** (întreprinderile mari) să utilizeze o **gamă mai largă de tehnologii IT și soluții de securitate** decât IMM-urile. Acest lucru este de așteptat, deoarece companiile mari au operațiuni mai complexe (care necesită automatizare, aplicații enterprise, interconectare cu partenerii etc.) și, în același timp, au resurse mai consistente pentru investiții IT. În schimb, **IMM-urile**, deși constrânse de bugete, încep treptat să adopte tehnologii mai avansate pe măsură ce devin mai accesibile, semn că există o **creștere a digitalizării,** inclusiv

în rândul companiilor mijlocii din sectorul alimentar. Acest progres lent, dar sigur, indică faptul că tot mai multe IMM-uri sunt conștiente de importanța tehnologiei (inclusiv a securității) pentru competitivitate.

- **Dimensiune vs. externalizare de securitate:** Companiile mari tind să **externalizeze** mai multe componente de securitate cibernetică (de exemplu, un producător cu mii de angajați poate utiliza un centru de operațiuni de securitate externalizat), în timp ce IMM-urile se bazează în mare parte pe eforturi interne sau deloc. Companiile mijlocii par să aleagă frecvent modelul mixt (păstrează managementul de bază intern, dar externalizează anumite servicii specializate). Această distribuție subliniază nevoia de oferte de securitate specifice categoriei: IMM-urile ar putea beneficia de servicii grupate externalizate sau platforme ușor de utilizat (din cauza lipsei de personal dedicat), iar companiile mari pun accentul pe integrarea furnizorilor în strategia lor complexă de securitate.
- **Regiunea geografică vs. adoptarea tehnologiei:** Diferențele regionale identificate în profilul respondenților se reflectă și în gradul de adoptare a soluțiilor avansate. În regiunile dezvoltate, cum ar fi **București-Ilfov** (și parțial în centru sau în vest), companiile au acces ușor la furnizori de servicii IT și la o infrastructură mai bună, ceea ce duce la o **adoptare mai mare a tehnologiilor de ultimă** generație și a serviciilor externalizate. De exemplu, multe companii din București menționează utilizarea serviciilor cloud sau colaborarea cu consultanți locali de securitate, în timp ce în regiuni precum Sud-Est sau Nord-Est, companiile se bazează aproape exclusiv pe propriile echipe IT și pe soluții tradiționale. Astfel, **regiunile mai puțin dezvoltate tehnologic** au un profil de risc diferit: tind să fie mai expuse la amenințări comune (din cauza predominanței soluțiilor de bază și a lipsei de specialiști), în timp ce companiile din regiunile avansate se confruntă cu un spectru mai divers de amenințări (fiind ținte pentru atacuri mai sofisticate, în funcție de tehnologiile utilizate).
- **Regiune vs. riscuri percepute:** Un rezultat interesant al analizei calitative indică faptul că respondenții din zone foarte digitalizate (de exemplu, București) au menționat îngrijorări cu privire la amenințări complexe, cum ar fi **atacuri ransomware avansate**, spionaj industrial sau atacuri asupra lanțului de aprovizionare, în timp ce respondenții din regiunile mai puțin dezvoltate au menționat mai des probleme "de bază" – cum ar fi **phishing-ul regulat** sau lipsa competențelor IT interne. Acest lucru sugerează o **conștientizare diferențiată**: acolo unde companiile au fost deja expuse unui mediu cu atacuri mai complexe, percepția riscului este mai acută și nuanțată, în timp ce în alte părți predomină în continuare o atitudine de "ceva grav nu ni se poate întâmpla, suntem mici".

Analizele pentru Bulgaria arată diferențe semnificative între organizații în ceea ce privește deciziile și măsurile de securitate cibernetică adoptate. Un aspect cheie este modul în care este gestionată funcția de securitate cibernetică: internă (cu personal propriu) sau externalizată (prin subcontractare). Rezultatele arată că există trei situații principale:

- Organizații care gestionează securitatea exclusiv intern – în aproximativ 50% din cazuri, companiile se bazează pe personal IT propriu pentru a asigura securitatea (instalare programe antivirus, firewall, întreținere de securitate etc.), fără a utiliza servicii externe.
- Organizațiile care externalizează complet serviciile de securitate cibernetică – reprezentând aproximativ 37% dintre respondenți, au contracte cu furnizori specializați care se ocupă de protecția infrastructurii lor.

- Organizațiile care aplică o abordare hibridă (mix de specialiști interni și externi) – aproximativ 13% dintre respondenți folosesc o combinație: mențin unele responsabilități de securitate internă, dar externalizează anumite servicii critice.

În ceea ce privește tehnologiile de securitate implementate, datele din Bulgaria arată că **principalele măsuri sunt:**

- Aproape toate organizațiile raportează că folosesc software antivirus pe stațiile lor de lucru – aproximativ 95% au confirmat că toate computerele și laptopurile lor sunt protejate de soluții antivirus actualizate. Acest lucru arată că în majoritatea cazurilor este asigurat un nivel minim de protecție a endpoint-urilor.
- În ceea ce privește firewall-urile de rețea: aproximativ 53% dintre organizații au o astfel de soluție (sub formă de hardware dedicat, soluție software sau serviciu cloud). O parte semnificativă - 47% - indică faptul că nu au deloc un firewall.
- Backup date: 63% dintre companii fac în mod regulat copii de rezervă a datelor importante, local sau în cloud, asigurându-se astfel că își pot restaura datele în caz de incidente (defecțiuni sau atacuri ransomware).
- Alte soluții de securitate menționate: sisteme de control al accesului (inclusiv controlul domeniului/directorului activ în cazul companiilor mai mari), soluții de securitate a e-mailului (de exemplu, filtre anti-spam, gateway securizat de e-mail), instrumente IDS/IPS pentru detectarea intruziunilor în rețea și, într-o măsură mai mică, soluții de prevenire a pierderii datelor (DLP) sau WAF (Web Application Firewall) pentru protejarea aplicațiilor web publice.

Cu toate acestea, adoptarea acestor tehnologii de securitate mai avansate (IDS/IPS, DLP, WAF etc.) este inegală: companiile mari le implementează, în timp ce întreprinderile mici și microîntreprinderile tradiționale din sectorul alimentar sunt de obicei limitate la programe antivirus, firewall-uri și backup-uri. Principalul motiv poate fi legat de costul și expertiza necesară - multe întreprinderi mici consideră că setul minim de măsuri este suficient și nu au personalul sau bugetul pentru soluții de întreprindere. Acest lucru evidențiază potențiala expunere la amenințări a unei părți semnificative a sectorului: atacatorii pot profita de lipsa de protecție avansată pentru a lansa atacuri.

Pe de altă parte, externalizarea securității către companii specializate oferă acces la expertiză și tehnologie de ultimă generație (monitorizare 24/7, threat intelligence, răspuns rapid), dar uneori vine cu provocări. Respondenții care au ales să externalizeze activitățile menționează beneficii precum audituri periodice de vulnerabilitate și consultanță, dar recunosc și riscurile asociate: dependență, posibile întârzieri în răspuns din cauza acordurilor privind nivelul serviciilor și costuri pe termen lung care pot deveni semnificative.

În general, aceste analize subliniază necesitatea unor **politici și strategii care să țină seama de context**: sprijin pentru IMM-uri (și în special pentru cele din regiunile întârziate) pentru a-și spori capacitățile de securitate, oferind în același timp abordări avansate pentru centrele economice în care digitalizarea aduce riscuri mai sofisticate. Fără o atenție diferențiată, decalajul de securitate cibernetică dintre diferitele categorii de organizații din sectorul alimentar se poate adânci.

Segmentarea organizațiilor și profilurile de maturitate cibernetică

Pe baza caracteristicilor analizate (dimensiune, tehnologii utilizate, nivel de externalizare etc.), am identificat trei **segmente principale de organizații** din punct de vedere al maturității securității cibernetice:

1. **Segmentul IMM-urilor cu soluții de bază** include microîntreprinderi și întreprinderi mici (dar și unele mijlocii) care utilizează în principal soluții IT și de securitate de bază. Aceste organizații au infrastructuri relativ simple (computere personale, rețea locală, eventual un site web) și se bazează pe licențe antivirus sau de bază gratuite, firewall-uri încorporate în routerele comerciale și backup ocazional. Nu au personal de securitate specializat și, în caz de nevoie, deleagă sarcini IT administratorului de sistem sau unei companii de asistență generală. Acest segment este cel mai **vulnerabil la atacuri comune** și are vizibilitate limitată asupra amenințărilor.

2. **Segmentul organizațiilor mijlocii cu un mix de soluții interne și externe:** aici găsim companii mijlocii și câteva companii mari care au adoptat o abordare hibridă – au dezvoltat anumite capabilități intern (ex. un departament IT cu 1-2 persoane cu o anumită expertiză în securitate) dar folosesc și servicii externe pentru aspecte critice (audit, monitorizare, conformitate). Aceste organizații au implementat deja măsuri de securitate standard (AV, firewall, backup regulat, politici de parolă) și încearcă să țină pasul cu noile cerințe (de exemplu, implementarea autentificării cu mai mulți factori acolo unde este posibil sau segregarea rețelei pentru sistemele de producție). Nivelul lor de maturitate este **mediu**, este prezentă conștientizarea riscurilor, dar adesea capacitatea de răspuns și prevenire este limitată de resurse. Acestea reprezintă cel mai dinamic segment, putând evolua pozitiv dacă beneficiază de îndrumare și sprijin.

3. **Segmentul organizațiilor mari, avansate din punct de vedere tehnologic** include companii mari (și câteva companii mijlocii) care au investit masiv în tehnologie și securitate. Aceștia folosesc soluții avansate (sisteme ERP interconectate, SCADA pentru automatizare industrială, IoT pentru trasabilitatea produselor), au implementat măsuri de securitate de ultimă generație (IDS/IPS, SIEM, instrumente de monitorizare a integrității, echipe sau servicii de răspuns la incidente) și de obicei externalizează servicii critice către furnizori de top (de exemplu, servicii SOC, teste anuale de penetrare, consultanță în conformitate). Acest segment are o **viziune proactivă** asupra securității, integrând-o ca parte a managementului riscului organizațional. Cu toate acestea, nici aceste companii nu sunt invulnerabile – complexitatea ridicată a infrastructurii și dependența de parteneri externi deschid alți vectori de risc (de exemplu, atacuri asupra furnizorilor terți, erori de configurare în sisteme complexe etc.).

Această **segmentare** este utilă pentru a înțelege diversitatea sectorului alimentar în ceea ce privește securitatea cibernetică. În același timp, poate ghida furnizorii de soluții IT&C să-și personalizeze **oferta**: de la pachete simple, la cheie pentru segmentul 1 (care are nevoie de soluții ușor de implementat și low-cost) până la servicii specializate pentru segmentul 3 (care are nevoie de expertiză de nișă și integrare complexă). Astfel, inițiativele de îmbunătățire a securității în sector ar trebui calibrate în funcție de segmentul țintă.

Din punct de vedere sectorial, este demn de remarcat faptul că există diferențe de accent între industrii, chiar și atunci când vorbim de securitate cibernetică. Profilarea sectorială sugerează că

sectoarele industrial și al transporturilor (incluse parțial în sondaj) au nevoi extrem de critice în materie de securitate cibernetică (din cauza dependenței de sistemele de control industrial și de logistica just-in-time), în timp ce **sectorul alimentar**, deși devine din ce în ce mai digitalizat, pune încă un accent puternic pe **întreținerea și operaționala** IT de bază sprijin, văzând securitatea ca pe o componentă de sprijin mai degrabă decât ca pe una strategică. Acest lucru nu înseamnă că companiile alimentare ignoră securitatea, ci că, în comparație cu alte sectoare, investițiile și preocupările lor se concentrează în continuare pe menținerea sistemelor în funcțiune (timp de funcționare, servicii IT) și mai puțin pe protejarea împotriva amenințărilor cibernetice complexe. Această constatare poate ghida adaptarea mesajelor de conștientizare: de exemplu, prin evidențierea legăturii directe dintre securitate și **continuitatea afacerii** (evitând oprirea producției sau distribuției), poate capta mai bine atenția factorilor de decizie din industria alimentară.

Principalele riscuri și amenințări cibernetice identificate

Întrebările deschise din sondaj, coroborate cu discuții și analize, au făcut posibilă identificarea unui set de **riscuri cibernetice majore** care privesc (sau afectează) sectorul alimentar. Rezumând răspunsurile și efectuând o analiză a termenilor menționați de respondenți, apar următoarele probleme centrale:

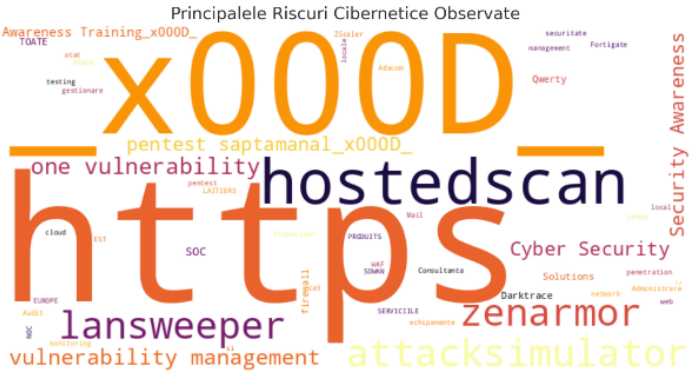

Figura 6. Norul de cuvinte.

- **Vulnerabilități tehnologice și lipsa actualizărilor:** Multe organizații au citat **Vulnerabilităţi** (sisteme de operare, aplicații utilizate sau echipamente industriale) ca sursă de risc. În special, **neaplicarea actualizărilor de securitate și a corecțiilor la timp** a fost semnalat ca o problemă – fie din cauza lipsei de timp/personal, fie din cauza fricii de a întrerupe producția prin actualizări. Astfel, software-ul învechit și echipamentele mai vechi (sisteme vechi) rămân în funcțiune, creând o suprafață de atac cunoscută pentru hackeri. Acest aspect este agravat de companiile care folosesc sisteme SCADA vechi sau software personalizat, pentru care actualizările sunt rareori sau dificil de aplicat.
- **Lipsa protecțiilor avansate:** Mulți respondenți au indicat că nu au soluții avansate de protecție (cum ar fi firewall-uri de ultimă generație, sisteme de detectare a intruziunilor, mecanisme de monitorizare continuă), menționând în mod explicit absența lor ca fiind o vulnerabilitate. Au fost întâlnite fraze precum *"nu avem un firewall dedicat, doar ceea ce oferă routerul"* sau *"folosim doar antivirus gratuit, nimic avansat"*. Această **lipsă de protecție avansată** este corelată cu constrângerile bugetare sau cu credința greșită că aceste companii nu ar fi ținte de interes pentru atacatori.
- **Breșe de securitate și scurgeri de date:** Teama de **breșe de date** (compromiterea informațiilor de afaceri sau a datelor personale ale clienților) este prezentă, chiar dacă nu toate companiile au experimentat așa ceva. În sectorul alimentar, încălcările pot viza date privind rețetele/formulele de producție, contractele cu furnizorii sau datele de identificare a clienților.

O încălcare majoră poate duce la **pierderi financiare, sancțiuni legale (dacă implică date cu caracter personal, conform GDPR) și pierderea încrederii** din partea partenerilor și consumatorilor. Deși mai puțin mediatizate, au existat incidente de acest tip – de exemplu, un exemplu ipotetic dat de un respondent: *"scurgerea detaliilor contractelor cu furnizorii ne-ar putea pune într-o situație nefavorabilă în negocierile viitoare"*. Acest lucru arată conștientizarea impactului reputațional și competitiv al securității informațiilor.

- **Atacuri de phishing și inginerie socială:** Aproape toți respondenții sunt conștienți de **atacurile de phishing** – e-mailuri frauduloase care încearcă să păcălească angajații să dezvăluie acreditări sau să descarce programe malware. Acest tip de amenințare este perceput ca fiind foarte comun. Sectorul alimentar, care nu are neapărat angajați IT foarte bine pregătiți, este vulnerabil la **erori umane**. Un scenariu comun menționat: atacatorii care se dau drept furnizori prin trimiterea de facturi false sau link-uri către pagini de phishing, cu scopul de a obține acces la sisteme interne sau plăți frauduloase. Educația angajaților despre phishing este adesea insuficientă, ceea ce înseamnă că acest risc rămâne ridicat.
- **Atacuri malware și ransomware:** Din ce în ce mai multe organizații din sector au auzit sau chiar au suferit atacuri ransomware – în care datele sunt criptate de atacatori, care apoi cer o recompensă. Impactul ransomware-ului în industria alimentară poate fi deosebit de grav, deoarece oprește producția și distribuția (orice oră de nefuncționare poate duce la pierderea loturilor de alimente perisabile). Un respondent a dat exemplul unui depozit frigorific: *"ransomware-ul care ne-ar bloca sistemele ar însemna că nu mai putem gestiona stocurile frigorifice, riscăm să pierdem bunurile"* – scenariu confirmat și de incidente reale care s-au întâmplat la nivel internațional. În general, atacurile malware (inclusiv virușii clasici și troienii) sunt văzute ca o amenințare constantă, împotriva căreia multe companii se bazează doar pe antivirus standard, ceea ce nu este întotdeauna suficient dacă angajații nu sunt vigilenți.
- **Riscuri în lanțul de aprovizionare digital:** Unele firme, în special cele mai mari, și-au exprimat îngrijorarea cu privire **la securitatea partenerilor și furnizorilor** cu care sunt integrate digital. De exemplu, un producător care se bazează pe un furnizor de soluții software pentru gestionarea stocurilor este vulnerabil dacă furnizorul respectiv este compromis. Atacurile asupra lanțului de aprovizionare sunt o amenințare emergentă: companiile alimentare pot fi afectate indirect de breșele partenerilor de logistică, transport sau IT. Un exemplu: dacă sistemele IT ale unui transportator de alimente sunt atacate, livrările pot fi întârziate sau redirecționate, afectând producătorii. De asemenea, echipamentele industriale inteligente (IoT) utilizate în fabrici pot servi drept vector de atac dacă furnizorii acestor echipamente nu le securizează corespunzător.

La prima vedere, **IMM-urile par a fi cele mai expuse** riscurilor de mai sus, din cauza resurselor limitate și a utilizării soluțiilor de securitate doar la nivel de bază. În schimb, companiile mari, deși ținte mai atractive pentru atacuri sofisticate, au de obicei și mijloace mai bune de protecție și răspuns. Diferențele regionale discutate mai sus își pun amprenta: regiunile mai puțin dezvoltate raportează incidente mai simple, dar frecvente (viruși, phishing de bază), în timp ce **amenințările diversificate și complexe** (atacuri APT, ransomware de ultimă generație) apar și în regiunile dezvoltate.

Este important de reținut că multe companii din sectorul alimentar se confruntă și **cu riscuri operaționale** care pot avea cauze cibernetice: de exemplu, o întrerupere sau o defecțiune a sistemului

de aer condiționat SCADA într-o instalație frigorifică poate fi cauzată de un atac cibernetic sau de o defecțiune IT și are consecințe directe (pierderi materiale). Astfel, riscurile cibernetice sunt interconectate cu riscurile operaționale în acest domeniu. Orice **întrerupere a activității** (fie că este cauzată de un atac sau de un incident tehnic) poate duce la nerespectarea termenelor limită de livrare, pierderi financiare și chiar reglementări privind siguranța alimentară (de exemplu, dacă "lanțul frigorific" este compromis).

În concluzie, **sectorul alimentar este expus unei game diverse de riscuri cibernetice**, amplificate de dependența tehnologică și de interconectarea operațională. În capitolul următor, vom plasa aceste constatări în contextul european mai larg, analizând perspectivele și recomandările ENISA privind securitatea cibernetică în sectorul alimentar, precum și evoluțiile recente ale reglementărilor și amenințărilor.

SECȚIUNEA 3. PERSPECTIVELE ENISA ȘI CONTEXTUL EUROPEAN

Pentru a înțelege mai bine poziția sectorului alimentar în peisajul european al securității cibernetice, vom examina informațiile și concluziile din **sursele ENISA** (Agenția Uniunii Europene pentru Securitate Cibernetică) și din alte rapoarte relevante. Această secțiune discută incidentele la nivel european, statisticile privind amenințările din sectorul agroalimentar, inițiativele de reglementare (cum ar fi NIS2) care includ în mod explicit industria alimentară, precum și previziunile privind evoluția riscurilor în viitor. Scopul este de a oferi un **punct de referință comparativ** pentru situația din România și de a identifica **bune practici** sau recomandări aplicabile.

Amenințări și incidente cibernetice la nivel internațional în industria alimentară

Potrivit datelor agregate de ENISA în ultimii ani, sectorul agroalimentar nu s-a numărat printre primele ținte ale atacurilor cibernetice raportate, dar importanța sa este în creștere. Rapoartele ENISA privind panoramul amenințărilor evidențiază că, în 2023, **sectorul agroalimentar a reprezentat aproximativ 1 % din totalul incidentelor de securitate cibernetică raportate** la nivelul UE. Acest procent poate părea mic în comparație cu sectoare precum finanțele sau sănătatea, dar nu trebuie interpretat ca o lipsă de risc – dimpotrivă, ENISA subliniază că **digitalizarea accelerată a agriculturii și a industriei alimentare, combinată cu o maturitate scăzută a securității, ar putea stârni un interes sporit al atacatorilor**. Cu alte cuvinte, pe măsură ce sectorul adoptă tehnologiile Industry 4.0 (automatizare, IoT, date cloud), suprafața de atac este în creștere, iar actorii rău intenționați ar putea profita de **lacunele de securitate existente**.

La nivel global, au existat deja o serie de **atacuri cibernetice majore asupra țintelor din sectorul alimentar și agricol**, care servesc drept lecții despre ce se poate întâmpla și la ce trebuie să fiți atenți:

- În 2021, un **important producător de carne (JBS Foods)** a suferit un atac ransomware care a afectat grav operațiunile din mai multe țări, forțând oprirea temporară a producției în SUA, Canada și Australia. Acest incident a atras atenția la nivel guvernamental, fiind considerat chiar probleme de securitate națională (protecția lanțului de aprovizionare cu alimente).
- Așa-numitul **"hack cu brânză"** – atacul asupra distribuitorului olandez de brânză din aprilie 2021 menționat mai sus – a demonstrat impactul direct pe piață al unui atac cibernetic rafturi goale în magazine, blocaje în lanțul logistic de la producători la comercianți cu amănuntul. Atacul a vizat sistemul ERP al distribuitorului, perturbând comunicarea cu magazinele și înregistrările de inventar.
- **Cooperative agricole și infrastructuri de irigații**: Tot în 2021, o cooperativă agricolă din Iowa (SUA) a fost lovită de un atac cibernetic care și-a dezactivat rețelele IT utilizate pentru a coordona hrănirea animalelor și livrările de cereale. Iar în 2023, un incident notabil a vizat sistemul automat de irigare al Israelului, provocând pierderi de recolte și trecerea la udarea manuală. Astfel de atacuri arată că **nu numai procesatorii de alimente sunt vizați, ci și fermele moderne și sistemele agricole inteligente**.
- **Atacuri demonstrative asupra echipamentelor agricole:** Un caz nou a fost compromisul tractoarelor John Deere în 2022, când hackerii au reușit să instaleze un joc video (DOOM) pe ecranele tractoarelor, în semn de protest împotriva securității slabe a acestor echipamente conectate. Deși nu a provocat daune directe, incidentul a evidențiat vulnerabilități în domeniul echipamentelor agricole și al conceptului de **agricultură** inteligentă.

Aceste exemple evidențiază diversitatea vectorilor de atac: de la ransomware-ul clasic orientat spre profit la **sabotarea proceselor fizice** (udare, aer condiționat, procesarea alimentelor) până la

exploatarea IoT agricolă. Pentru sectorul alimentar din România, lecțiile sunt că **amenințarea este reală și în creștere**, iar efectele pot fi majore (pierderi financiare, perturbări ale pieței, probleme de siguranță alimentară).

ENISA, împreună cu alte autorități (cum ar fi CISA în SUA), recomandă monitorizarea evoluției acestor amenințări și adaptarea continuă a strategiilor de securitate alimentară, tocmai pentru a **atenua riscurile în mod proactiv. Deși incidentele la scară largă sunt încă relativ rare în acest sector, tendința de bază este o creștere a nivelului atacurilor**, atât ca frecvență, cât și ca sofisticare.

O serie de factori specifici evidențiați și de experții ENISA și INCIBE (*Institutul Național Spaniol de Securitate Cibernetică*) într-o analiză dedicată industriei agroalimentare contribuie la vulnerabilitatea acestui sector:

- **Integrarea extinsă în lanțul de aprovizionare** face ca un atac asupra unei verigi să aibă un efect de domino. De exemplu, un producător depinde de furnizorii de logistică de transport și ambalaje – atacurile împotriva lor îl afectează indirect, dar sever. Această interconectare ridicată le face o țintă atractivă pentru atacatorii care doresc un impact maxim.
- **Maturitate scăzută în securitatea cibernetică**: sectorul alimentar este orientat în mod tradițional spre productivitate, costuri reduse și volum, ceea ce a dus la neglijarea securității cibernetice. Lipsa procedurilor și politicilor de securitate la multe companii le face mai susceptibile la atacuri. De asemenea, multe companii sunt **IMM-uri sau microîntreprinderi** fără personal de securitate dedicat, astfel încât vulnerabilitățile pot rămâne nerezolvate mai mult timp.
- **Adoptarea de noi tehnologii fără securitate adecvată**: Implementarea IoT, a senzorilor inteligenți și a automatizării în agricultură și producția alimentară a depășit adesea măsurile de protecție. Comunicațiile dintre dispozitive pot fi nesecurizate, configurațiile implicite – vulnerabile, serviciile expuse online – neprotejate și neprotejate. Pe scurt, sectorul se află încă într-o fază în care **tehnologia este introdusă înainte ca securitatea să fie pe deplin înțeleasă și** integrată.
- **Dependența de echipamente și software învechite**: multe fabrici alimentare folosesc utilaje vechi de zeci de ani, parțial modernizate cu sisteme IT. Aceste **tehnologii vechi** sunt dificil de securizat – nu acceptă actualizări, comunică prin protocoale vechi și pot fi ușor compromise. Pe de altă parte, echipamentele inteligente moderne, dacă nu sunt configurate corect, pot oferi atacatorilor puncte de intrare în rețeaua industrială.

În fața acestor realități, **ENISA recomandă un set de garanții adaptate sectorului alimentar** pentru a contracara atât amenințările actuale, cât și cele emergente. Vom detalia aceste recomandări în subcapitolul Recomandări, dar menționăm aici că prioritățile evidențiate includ: **instruirea personalului** (angajații fiind veriga slabă în multe atacuri, cum ar fi phishingul), **autentificarea cu mai mulți factori** acolo unde este posibil (mai ales la accesarea datelor sensibile), **backup-uri regulate** (pentru a atenua efectul ransomware), **politici și proceduri** de securitate clare (astfel încât angajații să știe cum să acționeze și să prevină incidentele), precum **și actualizarea și securizarea echipamentelor industriale** (întărire, închidere porturi neutilizate, segmentare rețele OT).

Cadrul european de reglementare (NIS2) și importanța sectorului alimentar

Din punct de vedere legislativ și politic, la nivelul Uniunii Europene a existat până de curând o anumită lacună în acoperirea sectorului alimentar în legislația privind securitatea cibernetică. Prima directivă NIS (Directiva privind securitatea rețelelor și a informațiilor, adoptată în 2016) s-a concentrat pe un set limitat de sectoare considerate esențiale (energie, transporturi, finanțe, sănătate, apă potabilă etc.), neincluzând în mod explicit industria alimentară în lista serviciilor esențiale. Cu toate acestea, unele state membre au extins lista la nivel național: de exemplu, **unele țări din UE au desemnat operatori din industria alimentară ca ESO (operatori de servicii esențiale)** sub

umbrela NIS1, recunoscând că securitatea lanțului alimentar este esențială. Cu toate acestea, la nivel european nu a existat o obligație uniformă pentru sectorul alimentar.

Lucrurile s-au schimbat odată cu actualizarea legislației. **Directiva NIS2**, adoptată la sfârșitul anului 2022 și care urmează să fie transpusă de statele membre (termenul limită octombrie 2024), extinde considerabil domeniul de aplicare. NIS2 **include în mod explicit industria alimentară ca un sector cu entități importante** din perspectiva securității cibernetice. Mai exact, directiva adaugă **producătorii, procesatorii și distribuitorii de alimente** pe lista sectoarelor reglementate, clasificându-i ca "entități importante" care vor trebui să implementeze măsuri de securitate și să raporteze incidentele. În plus, NIS2 elimină vechiul criteriu bazat pe importanța națională și îl înlocuiește cu un criteriu de dimensiune: **toate entitățile mijlocii și mari din lanțul de aprovizionare cu alimente vor fi acoperite de noua directivă (microîntreprinderile și întreprinderile mici fiind exceptate în mod implicit, cu excepția cazului în care un stat membru le declară în mod expres critice).**

Aceasta este o evoluție majoră: practic, marii procesatori de alimente, lanțurile de vânzare cu amănuntul de alimente, marile companii de distribuție de alimente din UE vor avea obligații legale stricte de securitate (evaluări ale riscurilor, măsuri tehnice și organizatorice, notificarea incidentelor semnificative etc.). Directiva NIS2 recunoaște astfel că **accesul la alimente este esențial pentru societate**, similar cu accesul la apă potabilă sigură, și că lanțul alimentar este suficient de dependent de rețele și de sistemele informatice pentru ca o perturbare cibernetică să aibă efecte grave.

Pentru România și Bulgaria, transpunerea NIS2 va însemna probabil identificarea și includerea marilor jucători din industria alimentară pe lista entităților esențiale/importante supravegheate de autoritățile competente de securitate cibernetică. Acest lucru ar trebui să conducă la o **îmbunătățire generală a nivelului de securitate**, deoarece societățile în cauză vor trebui să se alinieze la cerințele minime (care vor fi detaliate prin standarde și acte de punere în aplicare ale directivei).

Pe lângă NIS2, există și alte reglementări conexe care, deși nu sunt specifice industriei alimentare, au un impact asupra siguranței în acest sector:

- **Regulamentul general privind protecția datelor (GDPR)** – impune cerințe de securitate a datelor cu caracter personal. Orice companie alimentară care prelucrează date cu caracter personal (de exemplu, date despre angajați, clienți, parteneri) trebuie să implementeze măsuri tehnice și organizatorice adecvate pentru protecția acestor date. GDPR nu acoperă securitatea echipamentelor industriale dacă nu gestionează date cu caracter personal, dar principiul *"security by design"* promovat de GDPR încurajează în continuare producătorii de echipamente IT (inclusiv cele utilizate în agricultură/industria alimentară) să integreze securitatea în produs, ceea ce ajută și utilizatorii finali.
- **Legislația UE privind siguranța produselor** – de exemplu, Directiva privind echipamentele radio și reglementările delegate subliniază obligația producătorilor de a se asigura că echipamentele conectate la internet nu compromit rețeaua și că funcționarea lor este sigură. Acest lucru se referă și la echipamentele IoT utilizate în agricultură (senzori, camere inteligente, drone agricole) – producătorii lor trebuie să ia măsuri de securitate cibernetică, care, dacă sunt respectate, vor crește reziliența lanțului alimentar în ansamblu. Cu toate acestea, există încă lacune – de exemplu, Directiva privind mașinile care reglementează mașinile industriale acoperă mai mult siguranța fizică a mașinii, nu neapărat securitatea rețelei în care este integrată. Se discută despre revizuirea acestor legislații pentru a include în mod explicit cerințele de securitate cibernetică.
- **Inițiative de certificare și standardizare** – ENISA lucrează la sisteme de certificare de securitate cibernetică pentru diverse produse și servicii. În viitor, este posibil să vedem certificări pentru dispozitive IoT agricole sau pentru software utilizat în infrastructuri critice, ceea ce ar oferi un nivel de asigurare. De asemenea, standardele internaționale, cum ar fi ISO/IEC 27001 (managementul securității informațiilor) sau practicile industriei alimentare

(de exemplu, standardele de siguranță alimentară care ar putea încorpora elemente IT) vor juca un rol.

Una peste alta, **securitatea cibernetică a sectorului alimentar beneficiază de o atenție din ce în ce mai mare în cadrul legislativ și politic al UE**, trecând de la etapa "*neglijată" la cea "reglementată și monitorizată"*. Companiile noastre alimentare ar trebui să se pregătească activ pentru conformitatea cu noile cerințe (NIS2), ceea ce implică efectuarea de evaluări ale riscurilor, adoptarea unui set de politici de securitate, pregătirea procedurilor de răspuns la incidente și, nu în ultimul rând, **creșterea** gradului de conștientizare în rândul conducerii cu privire la importanța acestui subiect.

Privind în perspectivă: tendințe și amenințări emergente

ENISA, în exercițiul său de *previziune*, a încercat să anticipeze modul în care amenințările cibernetice ar putea evolua până în 2030. Unul dintre scenariile identificate ca având o probabilitate medie-mare și un impact semnificativ este direct legat de sectorul alimentar: **atacurile cibernetice care vizează perturbarea lanțului de producție alimentară**. Raportul ENISA *Foresight 2030* descrie posibilitatea unor amenințări, cum ar fi **inserarea de programe malware în sistemele de producție alimentară** sau atacurile de tip denial-of-service asupra infrastructurilor critice de procesare, cu scopul de a opri operațiunile sau chiar de a sabota siguranța alimentară. De exemplu, s-a speculat că atacatorii ar putea viza liniile automate de ambalare sau amestecare a ingredientelor, provocând defecțiuni care duc la **închiderea fabricilor sau la modificări neautorizate ale compoziției alimentelor**. Consecințele unor astfel de acțiuni ar putea fi dramatice: de **la penuria de** alimente și perturbări economice până la riscul de **contaminare intenționată a alimentelor** (dacă rețetele sau dozele sunt modificate cu rea intenție). ENISA avertizează că, pe fondul automatizării și robotizării tot mai mari a producției de alimente, aceste scenarii devin din ce în ce mai plauzibile și sunt necesare garanții serioase pentru a le preveni.

Un exemplu de risc viitor din analiza ENISA este cel numit *"Inserarea de malware pentru a perturba lanțul de aprovizionare cu producție alimentară",* unde se subliniază că atacatorii cu resurse medii și mari ar putea **manipula sistemele alimentare industriale** în moduri care au un impact fizic. De exemplu, un atac DoS asupra sistemelor de ambalare poate opri transportul produselor, iar compromiterea echipamentelor de producție poate duce la oprirea completă a operațiunilor unor unități de procesare a alimentelor. În cel mai rău caz, astfel de atacuri pot provoca **sabotaj alimentar** – de exemplu, modificarea setărilor unor mașini ar putea contamina produsele (imaginați-vă un scenariu extrem: schimbarea temperaturii într-un proces de pasteurizare sau sterilizare, făcând produsele nesigure). Deși aceste situații nu au fost încă raportate, pregătirea pentru ele este discutată în planurile de reziliență cibernetică.

În plus, **convergența dintre securitatea alimentară fizică și securitatea cibernetică** va deveni din ce în ce mai pronunțată. Pe lângă atacurile directe, pot exista și **campanii de dezinformare digitală** care vizează industria alimentară (de exemplu, răspândirea de știri false despre contaminarea unui produs, prin piratarea canalelor de comunicare ale unei companii), ceea ce reprezintă o altă fațetă a riscului într-o lume din ce în ce mai interconectată.

Pentru a contracara amenințările emergente, există discuții intense la nivel european cu privire la necesitatea **unor parteneriate public-privat** și a unui schimb de informații mai eficient în sectoare care au fost până acum mai puțin abordate, cum ar fi sectorul agroalimentar. Inițiative precum **ISAC (Centre de** Analiză și Schimb de Informații) specializate în alimentație sau agricultură pot ajuta companiile să rămână la curent cu tacticile și indicatorii de compromis recenti. Deja în SUA a fost înființat Food and Ag-ISAC, care emite rapoarte de amenințare pentru industria alimentară și agricultură, un model care ar putea fi replicat și la nivel european.

Un alt aspect al viitorului este rolul tot mai mare al **inteligenței artificiale** – atât ca instrument de apărare, cât și ca vector de atac. Pe de o parte, sistemele AI pot ajuta la detectarea anomaliilor în

procesele industriale alimentare (semnalizând posibile atacuri cibernetice sau defecțiuni), dar, pe de altă parte, atacatorii ar putea folosi AI pentru a identifica mai eficient vulnerabilitățile sau pentru a lansa atacuri automate la scară largă.

În concluzie, **perspectiva europeană evidențiază atât progresele – reglementări mai stricte și creșterea gradului de conștientizare – cât și provocările viitorului – amenințări din ce în ce mai sofisticate la adresa lanțului alimentar**. Sectorul alimentar începe să fie tratat ca un sector critic care trebuie protejat, iar companiile din domeniu vor trebui să evolueze de la o abordare reactivă (sau chiar pasivă) la una proactivă în gestionarea riscurilor cibernetice.

Concluziile

Sectorul alimentar se află într-un punct de inflexiune în ceea ce privește securitatea cibernetică. Pe de o parte, **digitalizarea accelerată** aduce beneficii economice și operaționale considerabile – automatizarea producției, managementul eficient al lanțului de aprovizionare, monitorizarea calității și trasabilitatea alimentelor – dar, pe de altă parte, **expune industria la amenințări cibernetice fără precedent**. Rezultatele studiilor noastre indică faptul că în România și Bulgaria companiile alimentare sunt din ce în ce mai conștiente de aceste riscuri, dar nivelul de pregătire și protecție variază foarte mult în funcție de dimensiune și resurse. IMM-urile din sectorul alimentar rămân vulnerabile la atacuri comune (malware, phishing) din cauza resurselor limitate și a utilizării măsurilor de securitate de bază, în timp ce companiile mari implementează soluții mai avansate, dar devin și ținte pentru atacuri mai complexe.

Am identificat **principalele riscuri cibernetice**: de la lipsa actualizărilor și a protecțiilor avansate, până la atacuri directe (phishing, ransomware) și indirecte (pe lanțul de aprovizionare). Faptul că multe dintre organizațiile analizate nu dispun de servicii de securitate dedicate arată că mai este încă un drum lung de parcurs în această industrie pentru a atinge un nivel satisfăcător de maturitate cibernetică. În același timp, exemplele internaționale ne arată că miza este foarte mare – un atac de succes poate opri producția, poate provoca pierderi de milioane de oameni și chiar poate pune în pericol siguranța publică. Din fericire, nu am găsit incidente majore în rândul companiilor analizate, dar absența incidentelor nu ar trebui să ducă la mulțumire, ci la **proactivitate**.

La nivel european, **sectorul alimentar a intrat oficial în centrul reglementărilor de securitate** (prin NIS2) și al analizei amenințărilor (ENISA evidențiază riscurile specifice agroalimentelor). Acest lucru înseamnă că și companiile din România și Bulgaria vor fi împinse de context să-și ridice standardele de securitate, ceea ce este un lucru pozitiv. Punerea în aplicare a unor strategii solide de securitate cibernetică în sectorul alimentar nu este importantă doar pentru întreprinderile individuale, ci devine o chestiune de **securitate națională și de reziliență a societății**: accesul continuu la alimente, prevenirea posibilelor crize alimentare cauzate de perturbările cibernetice, protecția consumatorilor împotriva posibilelor pericole.

Prezentul studiu oferă o privire integrată asupra situației actuale și a direcției evoluției. În concluzie, **protecția cibernetică a lanțului alimentar necesită o abordare combinată**: investiții în tehnologie (protecții avansate, infrastructură IT modernă), **educarea și conștientizarea angajaților**, consolidarea securității de-a lungul întregului lanț de aprovizionare (inclusiv parteneri) și cooperarea între companii și autorități. Numai printr-o astfel de abordare holistică sectorul alimentar își poate asigura **continuitatea operațională și poate preveni amenințările emergente**, menținând în același timp încrederea publicului în siguranța alimentară.

Sectorul alimentar al viitorului va fi unul de înaltă tehnologie, interconectat și eficient, dar pentru a fi sigur, **securitatea cibernetică trebuie să fie integrată organic în toate procesele**. Organizațiile din acest domeniu sunt încurajate să trateze securitatea nu ca pe o povară de conformitate, ci ca pe un **factor cheie în calitatea și sustenabilitatea** afacerii. În cele din urmă, securitatea cibernetică robustă

înseamnă produse alimentare livrate la timp, fără incidente care să compromită siguranța sau calitatea – care este exact promisiunea esențială pe care acest sector trebuie să o îndeplinească societății.

Corelații externe

Datele și rapoartele recente ale ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) confirmă și completează multe dintre observațiile extrase din studiul național realizat în România și Bulgaria. Următoarele grafice ilustrează modul în care tendințele europene se reflectă direct asupra situației din sectorul alimentar:

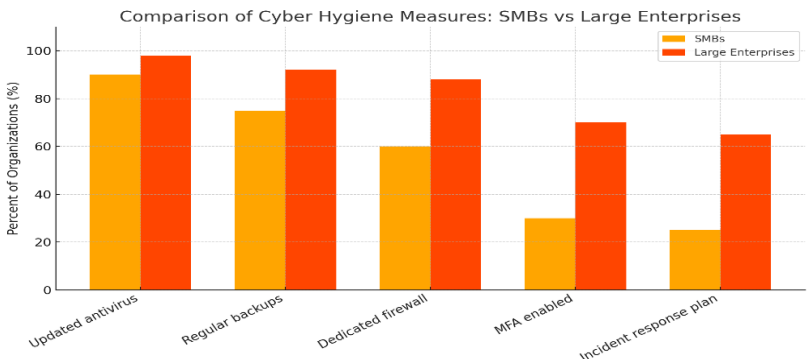

Figura 7. Comparația măsurilor de igienă cibernetică – IMM-uri vs întreprinderi mari.

IMM-urile aplică în principal măsuri de bază (antivirus, backup), dar rămân mult în urma companiilor mari în ceea ce privește autentificarea cu mai mulți factori (MFA) și planurile de răspuns la incidente. ENISA evidențiază aceeași problemă: lipsa igienei cibernetice de bază în IMM-uri este una dintre cele mai mari vulnerabilități structurale din UE.

Discrepanța dintre incidentele auto-raportate și realitatea estimată arată că IMM-urile, în special, **nu detectează sau nu recunosc multe dintre incidentele suferite**. ENISA avertizează că acest comportament duce la expunerea repetată la aceleași vulnerabilități.

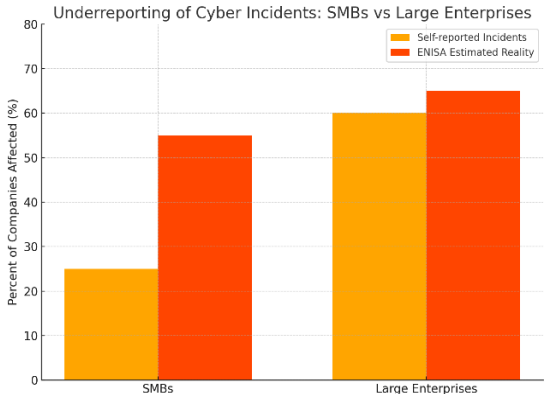

Figura 8. Subraportarea incidentelor cibernetice.

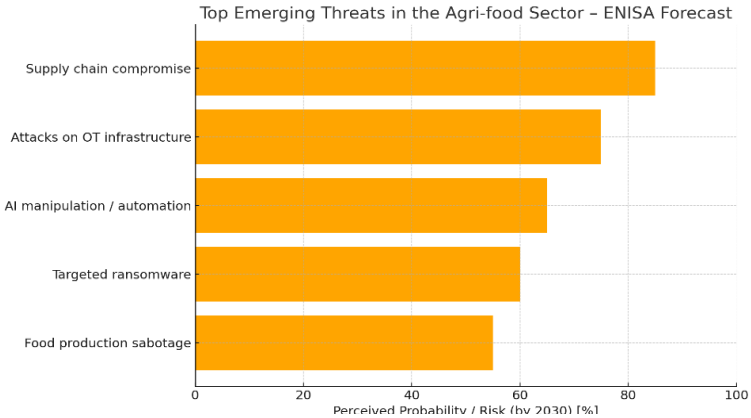

Figura 9. Principalele amenințări emergente până în 2030 (conform

Conform *PEISAJUL amenințărilor ENISA și previziuni 2030* Cele mai probabile și de impact pentru următorii ani includ: compromiterea lanțului de aprovizionare, atacuri asupra echipamentelor OT din industrie, ransomware specializat și utilizarea AI pentru atacuri. **Toate aceste riscuri sunt deja semnalate sau anticipate în sectorul alimentar din România și Bulgaria**, conform studiului nostru.

SECȚIUNEA 4. RECOMANDĂRI

Având în vedere constatările, formulăm o serie de recomandări pentru îmbunătățirea securității cibernetice în sectorul alimentar. Aceste recomandări se adresează atât companiilor din industrie (de la IMM-uri la corporații), cât și factorilor de decizie și partenerilor tehnologici:

1. Creșterea gradului de conștientizare și formare a personalului: Având în vedere că eroarea umană este un vector major de atac (de exemplu, phishing, atașamente rău intenționate), companiile ar trebui să investească în **programe regulate de formare** pentru angajați. Sesiunile de conștientizare a e-mailurilor de phishing, practicile sigure de utilizare a parolelor și manipularea dispozitivelor USB pot reduce dramatic riscul de incidente cauzate de neatenție. Cultura organizațională trebuie să promoveze **vigilența cibernetică** la toate nivelurile, de la operatorii fabricilor până la management.

2. Implementarea măsurilor tehnice esențiale (igienă cibernetică): Fiecare organizație, indiferent de dimensiune, ar trebui să se asigure că are cel puțin **măsuri de igienă cibernetică de bază**: soluții antivirus actualizate pe toate stațiile, **firewall de rețea** (inclusiv configurarea corectă a routerelor), **periodic** mecanisme de backup offline pentru date critice și actualizarea în timp util a tuturor sistemelor software. Aceste măsuri, deși par de bază, constituie prima linie de apărare și pot preveni majoritatea atacurilor nestructurate.

3. Adoptarea autentificării cu mai mulți factori (MFA): ori de câte ori este posibil (acces la e-mail, VPN, conturi privilegiate, platforme cloud), activați **autentificarea cu doi** factori. MFA adaugă un nivel suplimentar de securitate care poate opri atacurile chiar dacă parolele au fost compromise. Cu phishingul de acreditări galopant, MFA devine o necesitate minimă pentru protejarea conturilor.

4. Actualizarea și întreținerea sistemelor industriale: Pentru companiile cu echipamente de producție automatizate, se recomandă **auditarea securității infrastructurii OT (Operational Technology).** Aceasta include identificarea tuturor dispozitivelor conectate (inventar), aplicarea patch-urilor de securitate acolo unde furnizorii le oferă, **segmentarea rețelei** (separarea rețelelor de producție și de birou), închiderea serviciilor și porturilor neutilizate și modificarea acreditărilor implicite ale dispozitivului. Echipamentele vechi care nu pot fi actualizate trebuie izolate în rețea și monitorizate îndeaproape.

5. Dezvoltarea politicilor și procedurilor interne de securitate: Companiile ar trebui să dezvolte **politici clare de securitate cibernetică** – documente simple care să stabilească regulile de bază (utilizarea dispozitivelor, accesul la date, politicile de parolă, protocolul de raportare a incidentelor etc.). Aceste politici oferă angajaților **îndrumări privind comportamentul sigur** și reduc haosul în cazul unui incident. În plus, procedurile precum planurile de răspuns la incidente și planurile de continuitate a afacerii ar trebui să fie pregătite și testate prin simulări periodice, astfel încât organizația să reacționeze eficient în cazul unui atac.

6. Combinația de soluții interne și externe (model hibrid): IMM-urile care nu dispun de o capacitate internă suficientă ar trebui să ia în considerare **externalizarea serviciilor de securitate** către furnizori specializați (de exemplu, monitorizarea infrastructurii 24/7, administrarea firewall-urilor, servicii de răspuns la incidente). Un partener extern poate aduce expertiză pe care compania nu o are intern. Cu toate acestea, chiar și în acest caz, companiile ar trebui să păstreze un **minim de control și cunoștințe** interne – de exemplu, un ofițer de securitate internă (chiar dacă este cu jumătate

de normă) care ține legătura cu furnizorul și se asigură că politicile companiei sunt respectate. Acest lucru evită dependența totală de terți și menține reziliența pe termen lung.

7. Colaborarea în lanțul de aprovizionare: Companiile mari ar trebui să solicite partenerilor și furnizorilor lor să dețină standarde minime **de securitate** – de exemplu, clauze contractuale privind protecția datelor și notificarea incidentelor. În același timp, pot inițiа colaborări (cum ar fi **consorții sau alianțe sectoriale**) pentru a face schimb de informații despre amenințări și pentru a implementa soluții comune, în special la nivel local sau regional. De exemplu, companiile dintr-un parc industrial sau dintr-o asociație industrială pot împărți costul cursurilor de securitate sau pot construi împreună un centru local de monitorizare.

8. Respectarea cerințelor legale și a standardelor de bună practică: Întrucât Directiva NIS2 va impune obligații, companiile în cauză trebuie să se pregătească pentru **audituri de conformitate**. Chiar și cele care nu sunt obligate din punct de vedere juridic (de exemplu, IMM-urile sub prag) ar trebui să se inspire din cerințele NIS2 ca standard de **securitate**. De asemenea, se recomandă alinierea la standardele recunoscute (e.g. ISO 27001) pentru a structura sistemul de management al securității informațiilor. De asemenea, participarea la inițiative precum programul național de securitate cibernetică (dacă este cazul) sau accesarea fondurilor disponibile pentru digitalizarea securizată (de exemplu, fonduri europene pentru IMM-uri în domeniul securității cibernetice) poate accelera îmbunătățirile.

9. Monitorizarea evoluției amenințărilor și actualizarea strategiilor: Securitatea este un proces continuu. Companiile ar trebui să țină evidența rapoartelor privind amenințările (inclusiv cele sectoriale, cum ar fi rapoartele Food-ISAC sau buletinele CERT-RO) și să își actualizeze periodic evaluarea riscurilor. Pe măsură ce apar noi riscuri (de exemplu, amenințări la adresa tehnologiilor recent introduse, cum ar fi IA sau vehiculele autonome de transport intern), strategiile trebuie adaptate. Ideea este de a trece de la o abordare reactivă la una **proactivă și anticipativă** . Investiția în **capabilități de detectare timpurie** (monitorizarea jurnalelor, sisteme de alertare) poate face diferența în oprirea unui atac înainte ca acesta să provoace daune majore.

10. Planuri îmbunătățite de reziliență și continuitate: Având în vedere că nu toate atacurile pot fi prevenite 100%, este esențial ca întreprinderile să aibă planuri de rezervă pentru a-și continua activitatea în cazul unui incident cibernetic grav. De exemplu, menținerea procedurilor manuale de urgență (soluții) pentru funcționarea temporară fără IT, stabilirea **unor terenuri clare de recuperare** (RTO/RPO) pentru sistemele critice, precum și asigurarea faptului că backup-urile sunt testate și pot fi restaurate rapid. O bună **reziliență cibernetică** asigură că, chiar dacă un atac are parțial succes, compania va reveni rapid la funcționalitatea normală și va minimiza pierderile.

Punerea în practică a acestor recomandări va necesita efort și, în multe cazuri, o schimbare de mentalitate în rândul conducerii companiilor alimentare, care trebuie să vadă securitatea **cibernetică ca pe o investiție strategică, nu doar ca pe un cost sau o cerință de conformitate**. Pe termen lung, beneficiile – prevenirea incidentelor costisitoare, protejarea reputației, asigurarea continuității afacerii și conformitatea cu reglementările – depășesc cu mult investițiile inițiale. În contextul în care amenințările cibernetice nu vor dispărea, ci dimpotrivă, se vor intensifica, **doar organizațiile proactive și pregătite vor putea prospera fără** întreruperi.

Adoptarea unei poziții proactive față de securitatea cibernetică în sectorul alimentar va contribui nu numai la siguranța acestor întreprinderi, ci și la **siguranța alimentară a populației** și la încrederea generală în lanțul de aprovizionare cu alimente. Prin urmare, toate părțile interesate – industrie,

autorități, experți în securitate – trebuie să colaboreze pentru a consolida acest domeniu crucial al economiei. În era digitală, **securitatea cibernetică a devenit sinonimă cu calitatea și siguranța** în sectorul alimentar.

Bibliografie

- Burcu Yasar – *"Securizarea spațiului cibernetic european: este sectorul alimentar și agricol critic?"*, CiTiP Blog KU Leuven, 10 mai 2022. [Online]. Disponibil la: <https://www.law.kuleuven.be/citip/blog/securing-european-cyberspace-is-the-food-and-agriculture-sector-critical/#:~:text=Security%20rules%20also%20emanate%20from,or%20animals%20would%20presumably%20increase>.
- INCIBE-CERT (Spania) – *"Securitatea cibernetică în industria agroalimentară"*, 2023. [Online]. Disponibil: <https://www.incibe.es/en/incibe-cert/blog/cybersecurity-agri-food-industry>.
- ENISA – *"Prospective Cybersecurity Threats for 2030"* (raport 2024). <https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-extended-report>.
- Cibernetică industrială (2023). *"Legea privind securitatea cibernetică a fermelor și a alimentelor..."*. <https://industrialcyber.co/reports/food-and-ag-isac-cyber-threat-report-provides-actionable-intelligence-on-cyber-threats-ransomware-tactics/#:~:text=Food%20and%20Ag,on%20cyber%20threats%2C%20ransomware%20tactics>.
- Rapoarte și concluzii extrase din analiza internă pe un document anonimizat a datelor sondajului realizat în rândul organizațiilor din sectorul alimentar din România: profilul companiei, gradul de digitalizare, principalele riscuri percepute, diferențele pe regiuni și dimensiuni, nivelul de externalizare a securității etc.
- ENISA (2024). *Starea securității cibernetice în Uniune – Raport simplificat*.<https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union>.
- ENISA (2023). *Peisajul amenințărilor de securitate cibernetică 2023*.<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>.

TITLUL 2. MANUAL DE GESTIONARE A RISCURILOR DE SECURITATE CIBERNETICĂ A LANȚULUI DE APROVIZIONARE

Abstract

Această parte analizează riscurile cibernetice asociate lanțului de aprovizionare cu alimente din România și Bulgaria, în contextul implementării Directivei NIS2. În acest sens, sunt identificate amenințări majore, cum ar fi atacurile ransomware, vulnerabilitățile din sistemele IT/OT și expunerea întreprinderilor mici și mijlocii la procesul accelerat de digitalizare. Manualul propune un cadru de management al riscului cibernetic, aliniat la standardele internaționale (ISO/IEC 27005, NIST RMF), și recomandă măsuri tehnice și organizaționale, cum ar fi segmentarea rețelei, utilizarea soluțiilor EDR, autentificarea multi-factor (MFA) și planurile de continuitate a afacerii. De asemenea, sunt analizate cadrele legislative naționale – OUG nr. 155/2024 în România și modificările aduse Legii privind securitatea cibernetică din Bulgaria –, cu accent pe obligațiile de raportare a incidentelor și responsabilitatea managerială. Manualul subliniază importanța unei abordări integrate a securității cibernetice, axată pe conformitate, cooperare regională și reziliență operațională în sectorul agroalimentar.

SECȚIUNEA 1. INTRODUCERE

Gestionarea riscurilor de securitate cibernetică face parte din domeniul guvernanței de securitate cibernetică și este de o importanță fundamentală pentru modul în care riscurile de securitate cibernetică sunt gestionate la toate nivelurile, inclusiv riscurile de securitate cibernetică legate de lanțul de aprovizionare digital. Gestionarea riscurilor de securitate cibernetică trebuie să fie parte integrantă a setului de activități asociate unei entități economice și include interacțiunea cu părțile, inclusiv cu entitățile componente ale lanțului de aprovizionare digital (hardware și software).

Lanțul de aprovizionare cu alimente este infrastructura fizică prin care alimentele sunt produse, procesate, distribuite și livrate consumatorilor. Digitalizarea accelerată a sectorului alimentar în ultimul deceniu – de la sisteme automatizate în zona de producție la platforme IT pentru logistică, promovare și publicitate – a adus eficiență, creșteri substanțiale ale producției și vânzărilor, dar și o expunere sporită la riscuri de securitate cibernetică.

În ultimii ani, incidente semnificative de securitate cibernetică au evidențiat vulnerabilități specifice sectorului, vulnerabilități care au fost exploatate și au dus la materializarea riscurilor asociate acestor vulnerabilități, astfel, în 2021 un atac ransomware a paralizat un distribuitor de alimente din Olanda, blocând comunicarea cu depozitele și transportul și lăsând rafturile unui supermarket mare fără produse (cunoscut sub numele de "atacul cu brânză").

La scurt timp după aceea, cel mai mare producător de carne din lume a fost forțat să-și oprească operațiunile din SUA, Canada și Australia din cauza unui alt ransomware. De asemenea, companii de top din industria alimentară – cum ar fi Campbell Soup, Dole Foods, Heineken sau Krispy Kreme – au căzut victime recentelor atacuri cibernetice. Aceste exemple demonstrează în mod clar că sectorul agroalimentar nu mai poate trata securitatea cibernetică ca pe o problemă secundară, deoarece consecințele pot fi grave: pierderi financiare considerabile, întrerupere parțială sau totală a activității, afectarea siguranței alimentare și chiar a bunăstării animalelor.

Importanța strategică pentru societate a lanțului de aprovizionare cu alimente este comparabilă cu cea a altor sectoare esențiale (cum ar fi energia sau apa potabilă). Accesul la alimente sigure și disponibile în permanență este vital pentru bunăstarea populației și buna funcționare a economiei. Cu toate acestea, până de curând, politicile europene de securitate cibernetică nu au acoperit în mod explicit acest sector. Directiva NIS (2016) nu a inclus alimentele ca serviciu esențial la nivelul UE, deși mai multe state membre au înregistrat în mod voluntar anumite entități care își desfășoară activitatea în sectorul alimentar ca operatori de servicii esențiale (OEN). Această lacună administrativă a fost

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

remediată prin noua Directivă NIS2, care extinde domeniul de aplicare la sectorul alimentar (producători, procesatori și distribuitori de alimente), recunoscându-l ca fiind un "sector important" cu entități importante care necesită o protecție cibernetică sporită.

Acest manual abordează managementul riscului cibernetic în lanțul de aprovizionare digital din sectorul alimentar, cu accent pe situația concretă din România și Bulgaria în contextul inițierii procesului de implementare a Directivei NIS2. Această lucrare se adresează atât profesioniștilor (manageri IT, manageri de conformitate NIS, consultanți în securitate cibernetică), cât și mediului academic (studenți, masteranzi în securitate cibernetică și IT industrial). În paginile următoare, este prezentat un cadru teoretic solid împreună cu ghiduri și instrumente practice.

Conținutul manualului este structurat pe capitole tematice, acoperind de la aspecte legislative și de reglementare la procesele de gestionare a riscurilor, particularitățile securității cibernetice în lanțul de aprovizionare digital, planificarea continuității afacerii, gestionarea incidentelor de securitate cibernetică și cooperarea internațională, precum și bune practici și politici/proceduri model. Fiecare capitol extinde și aprofundează secțiunile inițiale, integrând atât perspective europene (ENISA, Comisia Europeană, standarde ISO, recomandări BSI/ANSSI/CERT etc.), cât și exemple concrete din România și Bulgaria, inclusiv instrumente utile (matrice de risc, checklist pentru evaluarea furnizorilor și serviciilor furnizate de aceștia, șabloane de politici, formulare de notificare a incidentelor de securitate cibernetică, planuri de continuitate).

Scopul introducerii este de a contura contextul și necesitatea unui astfel de manual. Complexitatea și sofisticarea tot mai mare a atacurilor cibernetice și interconectarea din ce în ce mai strânsă a lanțurilor de aprovizionare înseamnă că nimeni nu este scos din pădure. "Nimeni nu își asumă întregul risc. Dacă ai date sau sisteme valoroase, atacatorii vor căuta întotdeauna cea mai slabă verigă, adesea un partener plasat în lanțul de aprovizionare", subliniază experții. Prin urmare, organizațiile din industria alimentară trebuie să adopte o viziune integrată a securității cibernetice, care să includă atât protecția internă, cât și colaborarea cu furnizorii și distribuitorii. Manualul oferă îndrumări în acest sens, aliniate la cerințele Directivei NIS2 – noul standard european care impune o abordare sistematică a riscurilor cibernetice. În continuare, vom prezenta cadrul legal relevant, înainte de a trece la conceptele de management al riscurilor și la măsurile specifice sectorului alimentar.

SECȚIUNEA 2. CADRUL JURIDIC

Cadrul legislativ european – Directiva NIS2

Pentru a consolida reziliența cibernetică a infrastructurilor critice la nivelul Uniunii Europene, **în decembrie 2022 a fost adoptată Directiva (UE) 2022/2555 (NIS2)** privind măsurile pentru un nivel comun ridicat de securitate cibernetică în Uniune. Directiva NIS2 înlocuiește și actualizează primul domeniu de aplicare semnificativ al Directivei NIS, impunând cerințe de securitate sporite și sancțiuni mai dure pentru neconformitate. Unul dintre scopurile cheie ale Directivei NIS2 este tocmai **de a aborda riscurile legate de lanțurile de aprovizionare digitale**, o lecție învățată din valul de atacuri asupra furnizorilor și serviciilor terțe care au avut loc în ultimii ani.

Directiva NIS2 clasifică entitățile în două mari categorii de operatori: **entități esențiale** (în sectoare foarte critice) și **entități importante** (în sectoare critice). Sectorul alimentar – definit ca *fiind producția, prelucrarea și distribuția alimentelor* – este inclus în categoria sectoarelor critice, entitățile din acest domeniu de activitate fiind considerate entități importante. Aceasta înseamnă că toate entitățile economice mijlocii și mari (peste 50 de angajați sau cifră de afaceri de peste 10 milioane EUR) din lanțul de aprovizionare cu alimente intră automat sub incidența NIS2. (Spre deosebire de NIS1, unde statele au identificat ESO-urile pe baza unor criterii, NIS2 introduce așa-numita regulă a "plafonului de dimensiune" – includerea în funcție de dimensiune și sector, asigurând o acoperire uniformă a unui număr mult mai mare de operatori.)

Obligațiile impuse de NIS2 entităților esențiale și importante sunt substanțiale. Directiva prevede un set minim de măsuri de **gestionare a riscurilor de securitate** pe care fiecare entitate trebuie să le aplice, în conformitate cu principiul "**tuturor riscurilor**" (vizând orice tip de risc, nu doar specific cibernetic). Acestea includ efectuarea periodică de analize de risc și adoptarea de politici pentru securitatea sistemelor informatice; măsuri pentru **securitatea lanțului de aprovizionare digital** și a relațiilor cu furnizorii; programe de gestionare și actualizare a vulnerabilităților; utilizarea testelor de securitate (audit, pentesting) și criptografie adecvată; planuri de răspuns la incidentele de securitate cibernetică și asigurarea continuității operaționale. Directiva introduce, de asemenea, **responsabilitatea conducerii entităților economice** – conducerea entității este responsabilă pentru respectarea măsurilor de securitate cibernetică și poate fi sancționată personal în caz de neglijență gravă. Pentru un tratament uniform, NIS2 impune statelor membre să stabilească *sancțiuni armonizate*: nivelul maxim al amenzilor nu poate fi mai mic de **10 milioane EUR sau 2 % din cifra de afaceri totală** (se aplică entităților principale) sau **de 7 milioane EUR sau 1,4 % din cifra de afaceri** (pentru entitățile mari), oricare dintre acestea este mai mare. Aceste sancțiuni aliniate cu cele ale GDPR ilustrează importanța acordată securității cibernetice la nivel strategic.

Un aspect central al NIS2 este **raportarea incidentelor de securitate cibernetică**. Directiva stabilește un mecanism în două etape pentru notificarea incidentelor semnificative: inițial, transmiterea unei **alerte timpurii în termen de 24** de ore de la producerea incidentului (cu informații preliminare privind potențialele cauze rău intenționate și impactul transfrontalier); apoi, o **notificare detaliată în termen de 72 de ore**, cu o evaluare inițială a gravității și a impactului, inclusiv indicatori cunoscuți de compromis. În plus, în termen de o lună de la incident, entitatea trebuie să prezinte un **raport final** cu rezultatele investigației și măsurile de remediere. Scopul acestui regim de raportare pas cu pas este de a permite autorităților și rețelelor CSIRT să reacționeze prompt și să ofere sprijin, asigurând în același timp o analiză ulterioară aprofundată a incidentului. De menționat că Directiva NIS2 face distincție între entitățile esențiale și cele importante și în ceea ce privește supravegherea: entitățile critice sunt supuse unui **regim de supraveghere proactivă** (verificări periodice de către autorități), în timp ce entitățile importante vor fi supravegheate în principal **reactiv, post-incident**. Cu toate acestea, ambele categorii sunt obligate să respecte aceleași cerințe de securitate și pot primi sancțiuni similare dacă se constată o neconformitate gravă.

Tot la nivel european, Directiva NIS2 consolidează mecanismele de cooperare **între state**. Acesta prevede existența unui grup de *cooperare NIS* (pentru schimbul de politici și bune practici) și a *rețelei CSIRT* (pentru coordonarea operațională între echipele naționale de răspuns la incidente). NIS2 oficializează, de asemenea, *EU-CyCLONe* – rețeaua europeană de gestionare a crizelor cibernetice – menită să asigure coordonarea în incidente majore sau crize cu impact asupra mai multor state. Aceste aspecte ale cooperării transfrontaliere vor fi detaliate în capitolul dedicat, dar merită menționat faptul că directiva prevede, de asemenea, posibilitatea de a efectua **evaluări coordonate ale riscurilor privind lanțurile de aprovizionare critice** la nivelul UE. Un exemplu ar fi evaluările riscurilor efectuate la nivel european pentru infrastructura 5G – un model care poate fi extins la alte tehnologii critice pentru diferite sectoare.

Implementarea NIS2 în România – OUG 155/2024

În România, cadrul legal inițial al NIS a fost stabilit prin Legea nr. 362/2018, care a transpus Directiva NIS din 2016. Apariția NIS2 a necesitat actualizarea legislației naționale, materializată prin **Ordonanța de urgență nr. 155/2024**, adoptată la 30 decembrie 2024. OUG 155/2024 abrogă Legea 362/2018 (cu excepția unor prevederi tranzitorii) și stabilește un nou cadru pentru securitatea rețelelor și sistemelor informatice în spațiul cibernetic național civil, aliniat la cerințele extinse ale NIS2. Acest act normativ marchează un moment definitoriu în eforturile României de a-și consolida reziliența la amenințările cibernetice din ce în ce mai complexe.

Noul cadru legislativ clarifică aspecte care rămăseseră neclare în vechea lege și introduce elemente suplimentare în directiva europeană. În special, **domeniul de aplicare a fost lărgit considerabil:** OUG 155/2024 preia lista extinsă de sectoare critice/foarte critice din NIS2 (enumerate în anexele 1 și 2 ale ordonanței) și aplică *regula dimensiunii*, ceea ce înseamnă că **mii de companii românești** devin acum obligate să respecte noile cerințe. Dacă sub vechiul NIS erau identificate doar câteva zeci de operatori de servicii esențiale (ESO), acum practic orice organizație medie sau mare din sectoare precum energie, transporturi, finanțe, sănătate, apă, deșeuri, digital etc., dar și **din industria alimentară**, intră sub incidența OUG 155/2024. Astfel, lanțul de aprovizionare cu alimente – de la producătorii și procesatorii agroalimentari până la depozitare și distribuție angro – este recunoscut oficial ca un sector critic, entitățile din acest domeniu fiind clasificate ca entități importante care trebuie să implementeze măsuri de securitate și să raporteze incidentele conform legii.

Ordonanța stabilește termene și mecanisme clare de implementare. De exemplu, companiile în cauză trebuie să **se înregistreze** la autoritatea competentă (DNSC – Direcția Națională de Securitate Cibernetică, care acționează ca punct unic de contact NIS și autoritate națională) într-un anumit interval, iar DNSC va gestiona evidența entităților și incidentelor esențiale/importante. La momentul adoptării ordonanței, procesul de înregistrare nu era încă operațional, necesitând dezvoltarea de platforme și proceduri – autoritatea a anunțat că va emite ordine și metodologii secundare în prima parte a anului 2025 pentru clarificarea aspectelor practice. Până atunci, se aplică prevederile ordonanței, iar operatorii trebuie să înceapă procedurile de conformare.

Obligațiile de securitate și raportare prevăzute de OUG 155/2024 sunt în concordanță cu NIS2: efectuarea periodică a analizelor de risc, adoptarea politicilor de securitate internă, măsuri tehnice și organizaționale de protecție proporționale cu riscurile, gestionarea continuității și a incidentelor, notificarea incidentelor semnificative într-o anumită perioadă, cooperarea cu autoritățile și echipele CSIRT etc. **De asemenea, este prevăzută certificarea auditorilor de securitate informatică**, care va evalua conformitatea companiilor (proces care este în curs de actualizare față de regimul Legii 362/2018). Un element notabil este faptul că ordonanța introduce *unele măsuri suplimentare față de cadrul european*, pentru a se adapta la contextul local. De exemplu, responsabilitățile instituțiilor publice și procedurile interne de notificare sunt clarificate, iar DNSC este împuternicită să emită reglementări specifice (orientări, reglementări) pentru diferite sectoare, acolo unde este necesar. Amenzile pentru contravenție pentru încălcări reflectă nivelurile impuse de NIS2 (până la 2% din

cifra de afaceri globală), subliniind că securitatea cibernetică devine o obligație legală la fel de importantă ca protecția datelor cu caracter personal sau siguranța alimentară.

În concluzie, prin OUG 155/2024, România și-a aliniat legislația la Directiva NIS2, extinzând protecția cibernetică la lanțul alimentar. În 2025, autoritățile (DNSC) vor emite normele de punere în aplicare și vor începe să monitorizeze activ conformitatea. Entitățile din industria alimentară trebuie să trateze cu seriozitate aceste cerințe, investind în sisteme de securitate și risc, altfel riscă sancțiuni severe și, mai rău, incidente cu impact asupra populației.

Punerea în aplicare a NIS2 în Bulgaria – Legea privind securitatea cibernetică (actualizare)

Bulgaria a adoptat o lege privind securitatea cibernetică în 2018 care a transpus directiva inițială privind NIS, stabilind un cadru pentru identificarea operatorilor de servicii esențiale și reglementarea măsurilor de securitate. Legislația bulgară existentă prevede o structură de guvernanță cu un Consiliu de securitate cibernetică, un coordonator național și echipe de răspuns la incidente (CERT Bulgaria la nivel național), plus CSIRT sectoriale în domeniul energiei, finanțelor, transporturilor etc. Autoritățile de reglementare sectoriale au, de asemenea, rolul de a desemna operatorii esențiali și de a supraveghea respectarea cerințelor în aceste domenii. Până la implementarea NIS2, sectoarele cheie din Bulgaria includeau energia, transporturile, sectorul bancar, sănătatea, apa, infrastructura digitală etc., iar lista entităților OES era mai restrânsă.

În așteptarea NIS2, autoritățile bulgare au pregătit un **proiect de modificare a Legii privind securitatea cibernetică**, denumită uneori "Legea *privind securitatea cibernetică*". Acest proiect de lege a fost prezentat Parlamentului în iulie 2024, cu scopul de a transpune noile cerințe NIS2 în legislația națională. Până la termenul european (17 octombrie 2024), Bulgaria nu finalizase adoptarea amendamentelor, astfel că la acea dată transpunerea era încă nefinalizată, iar proiectul era în dezbatere parlamentară, ceea ce a condus la propunerea de **modificări substanțiale la** textul inițial. Procesul legislativ continuă spre sfârșitul anului 2024 și mijlocul anului 2025, deoarece legea modificată este de așteptat să fie adoptată în 2025, aliniind țara la standardele NIS2.

Modificările avute în vedere în noua lege bulgară includ extinderea domeniului de aplicare la mai multe sectoare și categorii de societăți. Practic, va trece de la lista restrânsă OES la includerea tuturor entităților mijlocii și mari în sectoarele critice și foarte critice definite de NIS2. Astfel, și în Bulgaria, industria alimentară (producători, procesatori, distribuitori de alimente) va intra oficial sub incidența legislației, ca *un sector critic* cu entități importante care trebuie să implementeze măsuri de securitate și să notifice incidentele semnificative. Noile norme vor impune **obligații sporite de gestionare a riscurilor și de raportare a incidentelor entităților în cauză**, similare OUG 155/2024 discutată mai sus. În plus, conducerea companiilor va fi trasă la răspundere pentru neconformitate, iar sancțiunile financiare vor fi majorate până la pragurile armonizate de NIS2 (milioane de euro sau procente din cifra de afaceri).

Până la intrarea în vigoare a modificărilor NIS2, Bulgaria continuă să aplice dispozițiile legislației existente (NIS1). Chiar și sub vechea lege, unele cerințe erau foarte stricte. De exemplu, **obligația de a raporta incidentele** în Bulgaria impune operatorilor esențiali să notifice echipa națională CSIRT **în termen de 2 ore** de la luarea la cunoștință a unui incident grav, urmată de un raport complet în termen de 5 zile lucrătoare. Acest termen de 2 ore pentru notificarea inițială este mult mai solicitant decât standardul NIS2 (24 de ore) și a fost stabilit tocmai pentru a asigura o reacție imediată la nivel național. Legislația bulgară impune, de asemenea, entităților să **coopereze pe deplin cu autoritățile și echipele de intervenție** în cazul unui incident, inclusiv prin furnizarea informațiilor necesare și, în cazul în care incidentul poate constitui o infracțiune, prin coordonarea cu organele de aplicare a legii (de exemplu, unitatea de criminalitate informatică). Asigurarea **continuității serviciilor**: întreprinderile trebuie să ia măsuri pentru a menține continuitatea serviciilor esențiale sau digitale în caz de perturbări cibernetice, prin planuri de urgență, concedieri și alte mijloace de reziliență. Nerespectarea obligațiilor atrage după sine sancțiuni: legislația bulgară prevede amenzi

administrative care, deși în forma veche erau mai mici (ordine de mii de euro), vor crește în regimul NIS2. Răspunderea civilă sau chiar penală poate fi angajată și pentru incidente grave cauzate de neglijență (codul penal bulgar prevede până la 8 ani de închisoare pentru infracțiuni informatice care afectează securitatea națională).

În concluzie, Bulgaria este în proces de actualizare legislativă pentru a implementa Directiva NIS2, un proces care implică extinderea obligațiilor de securitate cibernetică și la lanțul alimentar. Până la finalizarea noii legi, companiile bulgare din sector ar trebui să anticipeze cerințele care vor veni – practic similare cu cele din România și restul UE – și să înceapă să-și consolideze practicile de securitate. Autoritățile bulgare, conduse de Ministerul Guvernării Electronice (coordonatorul național NIS) și CERT Bulgaria, își vor intensifica eforturile de supraveghere și sprijin, asigurând tranziția către noul cadru. Prin armonizarea legislației, România și Bulgaria vor putea coopera mai eficient în securizarea lanțului transfrontalier de aprovizionare cu alimente, așa cum vom discuta în capitolele următoare.

SECȚIUNEA 3. MANAGEMENTUL RISCULUI

Managementul riscurilor este fundamentul oricărei strategii eficiente de securitate cibernetică. În esență, este un proces sistematic prin care o organizație **identifică, evaluează și tratează riscurile** care ar putea compromite atingerea obiectivelor sale, în acest caz continuitatea și integritatea lanțului de aprovizionare cu alimente. Standardele internaționale, cum ar fi **ISO 31000:2018**, oferă cadre de referință pentru managementul riscurilor în general, aplicabile și contextului securității cibernetice industriale. De asemenea, standarde specifice precum **ISO/IEC 27005** (managementul riscului de securitate a informațiilor) sau metodologii precum **EBIOS** (dezvoltat de ANSSI în Franța) sau **NIST SP 800-30** (SUA) detaliază pașii și tehnicile de evaluare a riscurilor în domeniul IT/OT. Directiva NIS2 impune entităților esențiale și importante să implementeze **politici de analiză a riscurilor și de securitate pentru sistemele informatice** care sunt actualizate periodic, ceea ce se traduce practic prin existența unui proces formal de management al riscurilor la nivelul organizației.

Procesul de management al riscului

Managementul eficient al riscurilor este un proces esențial în orice organizație, inclusiv în industria alimentară, unde amenințările pot afecta atât siguranța alimentară, cât și continuitatea afacerii. Procesul de management al riscurilor este o abordare sistematică prin care organizațiile identifică potențialele pericole, evaluează impactul și probabilitatea acestora, implementează măsuri de control și monitorizează continuu eficacitatea acestor măsuri. Acest proces este ciclic și iterativ, adaptându-se constant la schimbările din mediul organizațional și la apariția de noi amenințări.

Elementele clasice ale managementului riscului includ:

- **Identificarea riscurilor**

Primul pas este recunoașterea tuturor riscurilor potențiale care ar putea afecta atingerea obiectivelor organizației. În această etapă, se creează o listă (registru de risc) care include riscurile identificate, de la erori umane sau defecțiuni tehnologice până la atacuri cibernetice sau dezastre naturale.

- **Analiza riscurilor**

După identificare, fiecare risc este analizat pentru a înțelege cauzele acestuia, activele afectate, precum și modul în care s-ar putea manifesta. Analiza implică determinarea vulnerabilităților exploatabile și a factorilor care ar putea declanșa riscul. În contextul cibernetic, de exemplu, analiza riscurilor ar examina vectorii de atac (phishing, malware, exploit-uri) și gradul în care sunt expuse sistemele IT/OT.

- **Evaluarea riscurilor**

Următorul pas este evaluarea sau evaluarea riscurilor, adică estimarea impactului potențial și a probabilității de materializare a fiecărui risc. Pentru a determina nivelul de risc pot fi utilizate metode calitative (scale de la "scăzut" la "critic") sau cantitative (calcule financiare ale pierderilor așteptate). Scopul evaluării este de a prioritiza **riscurile** – adică de a determina care riscuri sunt inacceptabile și necesită tratament imediat, comparativ cu cele care pot fi tolerate pe termen scurt. În practică, multe organizații folosesc **criterii de acceptare a riscului** – de exemplu, un prag financiar sau de securitate peste care riscul trebuie tratat.

- **Tratamentul și controlul riscurilor**

Odată ce riscurile critice au fost identificate și evaluate, organizația dezvoltă și implementează **măsuri de tratare a riscurilor**. Există patru strategii generale de răspuns la risc: evitare (eliminarea activității care generează riscul, dacă este prea periculoasă), transfer (asigurare sau externalizare astfel

încât o terță parte să preia impactul financiar al riscului), atenuare (implementarea controalelor de securitate pentru a reduce probabilitatea sau impactul) și acceptare (asumarea riscului rămas, dacă este la un nivel tolerabil). De exemplu, confruntată cu riscul unui atac ransomware, o companie alimentară ar putea alege măsuri de atenuare (backup-uri offline, soluții antivirus avansate) și transfer (o poliță de asigurare cibernetică) în loc să accepte pasiv riscul.

- **Monitorizare și revizuire continuă**

Gestionarea riscurilor nu se oprește după punerea în aplicare a controalelor; monitorizarea continuă a eficacității acțiunilor întreprinse și reevaluarea periodică a peisajului riscurilor sunt esențiale. Mediul de securitate evoluează rapid – apar noi vulnerabilități, amenințările cibernetice se schimbă – așa că organizațiile trebuie să **revizuiască în mod regulat riscurile** și să ajusteze strategiile. Un proces eficient de management al riscurilor este unul dinamic, un "ciclu de viață" repetitiv în care monitorizarea feedback-ului duce la identificarea de noi riscuri sau la reevaluarea celor existente.

*Figura de mai sus ilustrează ciclul procesului de gestionare a riscurilor, inclusiv etapele de **identificare**, **analiză**, evaluare, tratament și **monitorizare continuă a riscurilor**. Acest ciclu se repetă periodic pentru a asigura îmbunătățirea continuă a securității.*

În industria alimentară, implementarea acestui proces general de management al riscurilor trebuie adaptată la specificul domeniului, care include atât infrastructuri IT clasice (rețele de calculatoare, baze de date), cât și tehnologii operaționale (echipamente industriale, SCADA/ICS) și cerințe stricte de siguranță alimentară. În continuare, vom aprofunda modul în care **riscurile cibernetice din sectorul alimentar** pot fi gestionate prin acest proces.

Riscuri cibernetice în sectorul alimentar: identificare, analiză și prioritizare

Industria agroalimentară s-a confruntat cu un val tot mai mare de amenințări cibernetice în ultimii ani, pe măsură ce digitalizarea și automatizarea proceselor s-au extins **"de la fermă la consumator".** Specificul sectorului alimentar – care combină lanțuri de aprovizionare complexe, sisteme de control al producției industriale și date sensibile despre rețete sau clienți – face ca riscurile cibernetice să fie unice. În această secțiune vom examina principalele amenințări digitale la adresa sectorului alimentar, precum și modalitățile de identificare și prioritizare a acestor riscuri prin cadre recunoscute (ex. ISO 27005, NIST RMF, OCTAVE).

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

Caracteristicile specifice ale riscurilor cibernetice în industria alimentară

O particularitate a acestui sector este interdependența dintre **tehnologia operațională (OT)** și tehnologia **informației (IT).** Fabricile de procesare a alimentelor utilizează sisteme SCADA și controlere logice programabile (PLC) pentru a automatiza amestecarea ingredientelor, ambalarea și conservarea condițiilor de mediu (temperatură, umiditate). Aceste sisteme, odată complet izolate de rețelele externe, sunt acum adesea conectate (direct sau indirect) la rețelele IT pentru a optimiza producția și lanțul logistic. Această convergență expune echipamentele industriale la atacuri cibernetice. De exemplu, *"percepția că există un spațiu de aer între sistemele alimentare automate și internet este adesea falsă – acestea sunt rareori complet izolate și au nevoie de actualizări regulate, ceea ce introduce vectori de atac",* după cum a subliniat un raport american. Un **fals sentiment de securitate** poate crește riscul, dacă managerii cred că sistemele lor industriale sunt protejate doar pentru că nu sunt aparent online.

În plus, sectorul alimentar funcționează adesea cu **termene foarte stricte** (de exemplu, produse perisabile care trebuie procesate și livrate rapid). Astfel, un atac cibernetic care oprește producția sau logistica chiar și pentru câteva zile poate duce la pierderi masive și chiar **penurie de alimente pe piață**. Acest lucru oferă atacatorilor un avantaj de presiune – companiile alimentare ar putea fi mai dispuse să plătească răscumpărări pentru a relua operațiunile afectate critic, de teamă să nu întrerupă aprovizionarea populației. În același timp, compromiterea datelor privind calitatea sau siguranța alimentară (de exemplu, rezultatele de laborator, certificările HACCP) poate avea consecințe asupra sănătății publice, ceea ce face ca anumite riscuri cibernetice să capete **o dimensiune de siguranță alimentară** în plus față de cea economică.

Exemple de amenințări cibernetice relevante: Printre cele mai frecvente riscuri cibernetice din industria alimentară se numără:

- **Atacuri ransomware asupra sistemelor IT și OT:** Ransomware-ul este considerat în prezent cea mai mare amenințare digitală pentru companiile din agricultură și alimentație. Un incident notoriu este cel suferit de compania JBS Foods în iunie 2021, când un atac ransomware a forțat închiderea tuturor fabricilor de procesare a cărnii de vită ale companiei din SUA (aproximativ 20% din aprovizionarea națională), JBS plătind o sumă de **11 milioane de dolari** infractorilor pentru a-și relua activitatea. Acest caz a arătat modul în care atacul cibernetic poate avea un impact sistemic asupra lanțului trofic. În 2023, un alt atac cibernetic a vizat Dole Food, perturbând operațiunile și ducând la **întârzieri și penurii de produse** în magazine. Statisticile recente confirmă tendința: numai în 2024, au existat 212 incidente de ransomware în sectorul alimentar și agricol, în creștere de la 167 în 2023. Astfel de atacuri blochează accesul la date critice (rețete, comenzi, planificarea producției) și pot paraliza atât producția cât și distribuția alimentelor la scară largă.
- **Atacuri asupra infrastructurilor industriale (SCADA/PLC):** O amenințare distinctă este infiltrarea rețelelor OT și preluarea proceselor industriale. Dacă un hacker obține acces la PLC-uri într-o fabrică de alimente, consecințele pot fi **catastrofale**. De exemplu, modificarea dozei aditivilor sau a parametrilor de sterilizare poate duce la **contaminarea produsului** sau la loturi întregi de alimente nesigure pentru consum. Imaginați-vă un scenariu în care într-o fabrică de conserve, un atacator crește temperatura sterilizatoarelor sub nivelul sigur: produsele rezultate ar putea părea normale, dar ar adăposti agenți patogeni. Astfel de riscuri combină aspectul cibernetic cu riscul tradițional pentru siguranța alimentară. În 2021, a existat chiar o încercare de otrăvire a unei rețele municipale de apă potabilă prin acces neautorizat la sistemul de control (în Oldsmar, Florida) – un incident care arată că atacurile asupra infrastructurii critice pot viza direct sănătatea publică.
- **Fraudă și phishing în context operațional:** Atacatorii exploatează adesea vectorul uman prin campanii de phishing sensibile la context. În companiile alimentare, un e-mail care pare a fi trimis de un furnizor de ambalaje sau de un partener logistic poate conține malware. Un

singur clic pe un atașament rău intenționat al unui angajat din departamentul de achiziții poate oferi intrușilor acces la rețea. Trebuie remarcat faptul că lanțul complex de aprovizionare crește suprafața de atac prin inginerie socială: există mulți parteneri, furnizori și clienți, atât de mulți vectori prin care un atacator se poate da drept "cineva de încredere". Un raport Verizon a arătat că **15% dintre breșele de securitate implică o terță parte** – adesea atacatorii compromit mai întâi un partener mai mic, apoi folosesc accesul acestora pentru a pătrunde în rețeaua țintă.

- **Atacuri ale lanțului de aprovizionare software și hardware:** Companiile alimentare folosesc soluții software de nișă pentru gestionarea fermei, a stocurilor sau a distribuției. Dacă acești furnizori de software sunt atacați (cum ar fi incidentul Blue Yonder din 2024, când un atac ransomware asupra unui furnizor de tehnologie a lanțului de aprovizionare a afectat clienții majori de retail), efectele se revarsă asupra tuturor clienților lor. De asemenea, dispozitivele IoT nesecurizate implementate în ferme sau fabrici (senzori de mediu, controlere de proces) pot acționa ca un **cal troian**: echipamentele compromise de la un furnizor pot introduce malware în rețeaua companiei alimentare atunci când sunt conectate. Astfel, **due diligence** in achizitia sistemelor IT/OT este critica – fiecare componenta noua trebuie verificata din perspectiva securitatii inainte de integrare.
- **Scurgeri de date sensibile și spionaj industrial:** Industria alimentară include și aspecte de proprietate intelectuală (rețete secrete, formule, procese tehnologice) care pot fi ținte pentru spionaj. Un atac cibernetic poate viza **furtul** rețetelor unui producător de băuturi sau al formulei unui conservant natural, ceea ce ar afecta avantajul competitiv. În plus, datele personale ale clienților (de exemplu, în comerțul cu amănuntul – numere de card, istoricul achizițiilor) pot fi furate dacă sistemele punctelor de vânzare sau bazele de date ale magazinelor sunt compromise. Aceste breșe provoacă daune semnificative imaginii lor, clienții pierzându-și încrederea dacă aud că datele lor au căzut în mâinile hackerilor. În noiembrie 2024, un lanț de supermarketuri din SUA (Stop & Shop) a suferit un incident cibernetic care a perturbat operațiunile de livrare și a dus la **rafturi goale** pentru produse proaspete în mai multe state – un exemplu care subliniază modul în care datele de vânzare cu amănuntul și sistemele IT sunt o parte integrantă a lanțului alimentar și pot provoca perturbări vizibile pentru populație.

Identificarea și prioritizarea riscurilor cibernetice – cadre de referință.

Pentru a gestiona eficient aceste amenințări, organizațiile alimentare pot apela la cadre de gestionare a riscurilor cibernetice recunoscute la nivel internațional. **ISO/IEC 27005** este un standard dedicat managementului riscurilor de securitate a informațiilor, care oferă îndrumări privind identificarea activelor informaționale, amenințărilor și vulnerabilităților, evaluarea riscurilor și tratarea acestora. Deși nu este specific sectorului alimentar, ISO 27005 poate fi aplicat pentru a structura o analiză a riscurilor cibernetice într-o fabrică de lactate, de exemplu, ajutând la identificarea tuturor elementelor (servere, PLC-uri, rețele wireless din depozit etc.) și a riscurilor asociate fiecăruia. Standardul recomandă stabilirea **de la început a criteriilor** de risc (ce nivel de impact este considerat grav, ce probabilitate este neglijabilă etc.), pentru a putea **clasifica ulterior riscurile** și a decide care necesită acțiune imediată.

Un alt cadru valoros este **NIST Risk Management Framework (RMF),** dezvoltat de Institutul Național de Standarde și Tehnologie din SUA. NIST RMF descrie un proces în 7 pași (Pregătire, Clasificare, Selecție a controlului, Implementare, Evaluare, Autorizare, Monitorizare) care integrează managementul riscurilor în ciclul de viață al sistemelor informatice. În contextul industrial (OT), FMR este adesea utilizat alături de linii directoare specifice, cum ar fi NIST SP 800-82 (securitatea sistemelor de control industrial) pentru a se asigura că riscurile cibernetice sunt identificate și atenuate încă din faza de proiectare a sistemelor de automatizare. De exemplu, prin aplicarea NIST RMF într-un siloz automat de cereale, managerii ar **clasifica sistemul** în funcție de impact (de exemplu,

disponibilitate foarte ridicată), **ar selecta controale adecvate** (de exemplu, segmentarea rețelei, controlul strict al accesului) și **ar monitoriza continuu** starea de securitate (prin audituri periodice).

Nu în ultimul rând, metodologia **OCTAVE** (Operationally Critical Threat, Asset and Vulnerability Evaluation) oferă o abordare axată pe evaluarea riscurilor de securitate la nivelul organizației și a activelor critice. OCTAVE subliniază implicarea personalului intern în identificarea amenințărilor și vulnerabilităților, evaluând atât aspectele tehnologice, cât și cele de proces și politici. Într-o companie alimentară, utilizarea OCTAVE ar însemna, de exemplu, organizarea de workshop-uri cu echipe mixte (IT, producție, calitate) pentru a cartografia posibile scenarii de atac (de la defectarea echipamentelor frigorifice până la furtul de date despre rețeaua de distribuție) și stabilirea **priorităților de tratament** în funcție de impactul asupra afacerii. Rezultatul ar fi un **plan de acțiune** care să combine măsuri tehnice (de exemplu, implementarea sistemelor de detectare a intruziunilor în rețeaua industrială) cu măsuri organizatorice (de exemplu, instruirea angajaților în phishing, revizuirea procedurilor de backup).

Concluzie intermediară

Riscurile cibernetice în sectorul alimentar sunt variate și pot provoca atât daune financiare, cât și probleme de siguranță alimentară și încredere publică. Prin aplicarea riguroasă a procesului de management al riscurilor – identificarea amenințărilor relevante, analizarea vulnerabilităților specifice (de la fabrica de procesare la supermarket), evaluarea impactului potențial și prioritizarea intervențiilor – organizațiile pot construi reziliență. Utilizarea cadrelor de referință precum ISO 27005, NIST RMF sau OCTAVE oferă **structură și consecvență** acestei abordări, asigurându-se că nicio problemă critică nu este trecută cu vederea. În capitolul următor vom explora mai detaliat **măsurile concrete de securitate cibernetică** care pot fi aplicate de-a lungul lanțului de aprovizionare cu alimente, ca parte a tratamentului riscurilor identificate.

Securitatea cibernetică în lanțul de aprovizionare cu alimente

Lanțul de aprovizionare agroalimentar este un ecosistem complex, care cuprinde producători de materii prime, procesatori, transportatori, distribuitori și comercianți cu amănuntul. Fiecare verigă din lanț – de la fermă la raft – se bazează din ce în ce mai mult pe tehnologie pentru eficiență și trasabilitate, deschizând noi suprafețe de atac pentru infractorii cibernetici. În acest capitol ne concentrăm pe o **abordare tehnică și operațională** a securității cibernetice în lanțul de aprovizionare cu alimente: vom descrie vulnerabilitățile specifice fiecărui segment al lanțului, posibilii vectori de atac, precum și măsurile de protecție recomandate (tehnologii, politici, audituri). De asemenea, vom evidenția bunele practici adaptate atât întreprinderilor mici și mijlocii (IMM-uri), cât și marilor operatori economici din industria alimentară.

Vulnerabilități și riscuri cibernetice în segmentele lanțului agroalimentar

Lanțul alimentar poate fi împărțit, simplificat, în patru segmente principale: **prelucrarea producției alimentare**, **transportul și logistica**, **distribuția angro** și **comerțul cu amănuntul** (retail). Fiecăruia corespund fiecăruia diferite tipuri de furnizori și operatori, dar toți se bazează pe tehnologii digitale interconectate. Vom analiza pe rând aceste segmente, evidențiind riscurile cibernetice specifice.

- **Producția și prelucrarea alimentelor (furnizori/procesatori)**

Aceasta include fabrici și instalații în care materiile prime agricole sunt transformate în produse alimentare finite (de la abatoare și fabrici de cârnați, până la conserve, produse lactate, brutării etc.). Caracteristicile acestui segment: prezența intensivă a **sistemelor de control industrial** (PLC, SCADA) care guvernează liniile de producție, roboți industriali, sisteme de ambalare și echipamente de siguranță (de exemplu, senzori pentru controlul calității). Vulnerabilitate specifică:

  - **Echipamente OT vechi sau învechite:** Multe fabrici folosesc echipamente cu cicluri de viață lungi (10-15 ani) care pot rula software învechit cu vulnerabilități cunoscute. De

exemplu, un *sistem SCADA* care controlează temperatura într-un cuptor industrial ar putea rula pe o versiune învechită, fără patch-uri și fără patch-uri de Windows, reprezentând o poartă de acces pentru malware.

- **Rețele insuficient segmentate:** Dacă rețeaua de producție este conectată la rețeaua IT corporativă fără segmentare, un atac care pornește de la un simplu computer din birou poate afecta direct mașinile din plantație. Un raport al experților din industrie subliniază că segmentarea rețelelor ICS (Industrial Control Systems) ar trebui să facă parte dintr-o strategie de securitate aprofundată pentru a preveni atacatorii să se deplaseze necontrolat în rețea. Lipsa segmentării permite unui adversar care a pătruns prin perimetrul clasic (firewall corporativ) să se deplaseze lateral în zonele critice OT.
- **Acces de la distanță nesecurizat** : Multe fabrici au opțiuni de acces de la distanță pentru întreținerea echipamentelor (furnizorii pot diagnostica mașinile de la distanță). Dacă aceste conexiuni VPN/RDP nu sunt protejate cu autentificare multiplă (MFA) și restricții stricte, acestea pot fi compromise. Cazuri reale arată că atacatorii profită de acreditările slabe reutilizate – cum a fost cazul la JBS, unde breșa inițială a avut loc după ce un angajat a folosit aceleași parole la locul de muncă și pe un site extern.
- **Eroare umană și lipsă de conștientizare:** Personalul de producție, concentrat pe obiectivele de volum și calitate, poate să nu fie suficient de instruit în practicile de securitate cibernetică. Un stick USB infectat introdus într-un computer industrial sau într-o stație de lucru tehnologică poate lansa un atac. Cultura securității este încă la început în multe fabrici alimentare, unde accentul istoric a fost pus pe siguranța muncii fizice și siguranța alimentară, nu pe securitatea IT.

- **Transport și logistică (furnizori de transport, depozitare)**

Acest segment include companii care transportă materii prime și produse finite, precum și depozite și centre logistice unde sunt depozitate și redistribuite mărfurile. Tehnologia joacă un rol major: **vehicule conectate** (camioane frigorifice cu telemetrie, GPS, senzori de temperatură în remorci), **sisteme de gestionare a flotei**, **depozite inteligente** (de exemplu, depozite automate cu roboți sau benzi transportoare controlate de computer). Vulnerabilități și riscuri:

- **Sisteme IoT nesecurizate:** Vehiculele de transport moderne au integrat IoT – de la senzori care monitorizează temperatura până la dispozitive care transmit poziția și starea în timp real. Aceste dispozitive, dacă nu sunt securizate (parole implicite, protocoale necriptate), pot fi piratate de la distanță. Un atacator care compromite senzorii unui camion frigorific ar putea opri sistemul de **răcire sau ar putea** modifica senzorii astfel încât șoferul să nu observe creșterea temperaturii, ceea ce duce la deteriorarea încărcăturii pe drum. În mod similar, accesul neautorizat la sistemul unui depozit poate permite ventilatoarelor să se oprească, crescând umiditatea și distrugând loturi de cereale depozitate.
- **Platforme IT logistice:** Întregul flux logistic este de obicei orchestrat de software specializat (sisteme de management al transportului, sisteme de management al stocurilor – WMS). Dacă aceste platforme sunt afectate de ransomware sau DDoS, operațiunile se opresc. Un exemplu ipotetic: un atac ransomware lovește sistemul central de gestionare a depozitelor unui lanț de supermarketuri, criptând baza de date a stocurilor și rutele de livrare; Rezultatul ar fi **întârzieri majore în livrări și rafturi neaprovizionate** până la restabilirea rezervelor. Astfel de atacuri s-au întâmplat chiar – de exemplu, atacul din 2024 asupra furnizorului de software Blue Yonder a perturbat lanțurile de aprovizionare ale comercianților cu amănuntul precum Sainsbury's, forțându-i să recurgă temporar la proceduri manuale.

- **Dependența de terți și integrarea acestora:** Transportul și depozitarea sunt adesea externalizate către firme terțe. Aceasta înseamnă legături IT între companii – schimb de date, portaluri comune, API-uri. Dacă oricare dintre acești parteneri este compromis, **atacatorii pot folosi conexiuni de încredere** pentru a pătrunde mai departe. Un exemplu concret: un atacator pătrunde în sistemul unei mici companii de transport, apoi folosește certificatele digitale furate de acolo pentru a accesa portalul unui producător important unde acea companie avea acces pentru comenzi. Atacurile prin lanțul de aprovizionare sunt în creștere (Verizon estimează că ~15% implică terțe părți), ceea ce face ca evaluarea securității să fie esențială atunci când se integrează (contractează) noi furnizori.
- **Interferența cu sistemele de navigație și comunicații:** Un aspect adesea trecut cu vederea este faptul că flotele logistice depind de GPS și de rețelele mobile. Atacatorii sofisticați ar putea folosi bruiajul GPS sau falsificarea pentru a dezorienta camioanele de livrare sau dronele sau pentru a intercepta comunicațiile radio necriptate. Aceste acțiuni sunt mai mult legate de securitatea comunicațiilor, dar devin parte a peisajului riscurilor cibernetice al logisticii alimentare.

- **Distribuție și angro (distribuitori, noduri regionale)**

Acest segment conectează producătorii și comercianții cu amănuntul, de obicei prin centre mari de distribuție, unde produsele din mai multe surse sunt consolidate, sortate și trimise în magazine. Din punct de vedere tehnologic, seamănă cu segmentul logistic (depozite mari, automatizate, sisteme IT de gestionare a stocurilor), dar are și particularități: volume mari de date de tranzacții, legături directe cu sistemele comercianților cu amănuntul pentru prognoza cererii și, uneori, sisteme **financiare** (facturare, EDI – Electronic Data Interchange cu furnizorii). Riscurile specifice includ:

- **Atacuri asupra datelor și sistemelor financiare:** Un distribuitor gestionează mii de facturi și plăți. Un atac Business Email Compromise (BEC) ar putea intercepta o plată importantă sau redirecționa fonduri (de exemplu, schimbarea contului bancar al unui furnizor în baza de date după un e-mail fraudulos). De asemenea, compromiterea sistemelor EDI poate perturba comenzile către producători, ceea ce are un efect direct asupra golirii stocurilor de pe raft dacă comenzile nu mai sunt transmise corect.
- **Infrastructură IT centralizată critică:** centrele de distribuție se bazează pe infrastructura IT centrală (servere, baze de date). Adesea există **un singur ERP** care coordonează întregul flux. Acest lucru devine un *singur punct de eșec* din perspectivă cibernetică – orice atac de succes aici (ransomware, sabotaj intern) poate opri complet capacitatea de a livra produse către sute de magazine. De aceea, planurile de continuitate (recuperare în caz de dezastru) și **backup-ul offline** sunt vitale la acest nivel.
- **Vulnerabilități fizice cu impact cibernetic:** centrele angro pot fi ținte pentru acces fizic neautorizat (intrus în depozit) care poate conecta un dispozitiv neautorizat la rețea sau poate fura un server din incintă. Controlul accesului fizic și monitorizarea video devin părți integrante ale securității cibernetice, deoarece un atacator determinat poate combina metode (fizice + cibernetice) pentru a exploata o organizație.

- **Comerț cu amănuntul (comerț cu amănuntul cu alimente**

Ultimul link, format din supermarketuri, hipermarketuri, magazine alimentare mici și platforme de comerț alimentar online. Tehnologiile implicate includ **sisteme moderne POS (Point of Sale)** și case de marcat, rețele Wi-Fi pentru clienți, aplicații mobile de cumpărături online, sisteme de fidelizare a clienților și infrastructură IT în magazine (terminale, chioșcuri de self-checkout etc.). Exemple de vulnerabilități și riscuri:

- **Compromiterea sistemelor POS:** Terminalele de plată din magazin și casele de marcat sunt adesea vizate de malware specializat (de exemplu, **malware POS** care extrage date din banda magnetică a cardurilor). Dacă retailerul nu menține aceste sisteme actualizate

și nu folosește criptarea end-to-end pentru tranzacții, infractorii pot fura **datele cardurilor de credit ale clienților** direct din memorie. Au existat breșe celebre în comerțul cu amănuntul (de exemplu, atacul asupra Target din SUA în 2013) care, deși nu sunt specifice alimentelor, arată ce expunere reputațională și financiară pot avea milioane de clienți.

- **Atacuri asupra infrastructurii digitale din magazine:** Pe măsură ce comerțul cu amănuntul devine omnicanal, magazinele fizice sunt integrate cu platforme online, aplicații mobile și sisteme de livrare la domiciliu. Un atac cibernetic poate implica **DoS (Denial of Service)** pe site-ul de cumpărături online al unui supermarket, paralizarea comenzilor online sau compromiterea aplicației mobile de scanare a produselor (dacă comunicarea cu serverul nu este sigură). De asemenea, deoarece multe magazine se bazează pe conexiuni VPN la centru pentru inventar și prețuri, ransomware-ul care afectează sediul central poate **bloca și magazinele fizice** (care nu mai pot scana produsele sau procesa plăți dacă nu pot accesa serverele centrale).
- **Riscuri pentru datele consumatorilor:** Comercianții cu amănuntul de produse alimentare colectează nume, adrese, istoricul achizițiilor (prin carduri de loialitate) și informații de plată. Aceste date sunt atractive pentru atacatori fie pentru revânzare pe piața neagră, fie pentru șantaj (de exemplu, un lanț de supermarketuri ar putea fi șantajat cu expunerea publică a datelor clienților). Un incident de referință a avut loc la **compania Krispy Kreme** în 2024, când un atac cibernetic a perturbat sistemul de comenzi online într-o perioadă de vârf, afectând clienții și veniturile. Chiar dacă nu a implicat furtul de date, cazul evidențiază dependența retailului de platformele digitale.

Sistem POS într-un supermarket modern – un exemplu de tehnologie digitală esențială în lanțul de aprovizionare cu alimente. Astfel de sisteme, dacă nu sunt protejate corespunzător, pot deveni ținte pentru atacatorii cibernetici, compromițând datele de plată ale clienților sau perturbând operațiunile de vânzări. Implementarea actualizărilor de securitate și segmentarea rețelei de magazine ajută la reducerea acestor riscuri.

Vectori de atac specifici lanțului de aprovizionare

Din exemplele de mai sus, reiese că multe riscuri se propagă prin legăturile dintre segmente. Două sectoare merită evidențiate:

- *Atacuri de la terți*: Fie că este vorba de un furnizor de materii prime, un transportator sau un furnizor de servicii IT, cea mai slabă verigă din lanț poate fi poarta. O breșă la un mic producător local care furnizează ingrediente poate oferi acces la sistemul unui procesor mare, dacă cei doi au sisteme interconectate pentru comenzi. De aceea, evaluarea **securității furnizorilor** și impunerea unor cerințe minime de securitate în contracte a devenit esențială în managementul lanțului de aprovizionare (vom detalia măsurile).
- *Atacuri asupra datelor și a sistemelor de încredere*: lanțul alimentar se bazează pe acuratețea datelor (de exemplu, date de testare HACCP, certificate de calitate sau chiar etichete de produse). Un atacator care reușește să falsifice sau să șteargă astfel de date poate provoca haos. De exemplu, dacă planul HACCP al unei fabrici (care indică puncte critice de control pentru siguranța alimentară) este furat și publicat, atacatorii ar putea identifica **punctele slabe** (așa cum arată exemplul expunerii planului HACCP menționat de TXOnetxone.com) sau ar putea șantaja compania cu dezvăluirea lor. Integritatea informațiilor din lanț (inclusiv trasabilitatea loturilor) este, prin urmare, o problemă de securitate cibernetică, nu doar una de calitate.

Măsuri de protecție cibernetică recomandate în lanțul agroalimentar

Având în vedere multitudinea de riscuri, companiile din sectorul alimentar trebuie să adopte o **strategie de apărare cibernetică** pe mai multe niveluri, aplicând principiul **apărării în profunzime**. Vom prezenta în continuare o serie de tehnologii cheie, politici și practici recomandate pentru a proteja lanțul de aprovizionare, de la producție la vânzare cu amănuntul:

- **Segmentarea și securizarea rețelelor OT și IT: După cum** am menționat, segmentarea rețelei este fundamentală. Practic, rețeaua IT corporativă (calculatoare, birouri, internet) trebuie să fie strict separată de rețeaua operațională OT (SCADA, PLC-uri, senzori din fabrică), permițând doar comunicațiile necesare prin gateway-uri securizate și firewall-uri industriale. Segmentarea limitează **răspândirea laterală** a unui atac – de exemplu, chiar dacă un PC desktop este infectat cu malware, nu ar trebui să ajungă să controleze cuptoarele sau liniile de îmbuteliere. Specialiștii ISA recomandă segmentarea ca parte a celor mai bune practici de securitate de secole în domeniul fizic și de decenii în IT, arătând că oferă un nivel de securitate mult mai robust decât o singură apărare perimetrală. În plus, **micro-segmentarea** în rețelele OT (zonarea și diviziunea celulară conform ISA/IEC 62443) poate chiar opri mișcarea unui atacator care a pătruns în OT – de exemplu, PLC-urile de ambalare sunt într-o zonă separată de PLC-urile de gătit, cu o comunicare minimă între ele, supravegheate și filtrate.
- **Soluții EDR (Endpoint Detection and Response):** EDR este o tehnologie care monitorizează activitatea pe stații de lucru și servere în timp real, pentru a detecta comportamente anormale (indicative de malware sau atacuri) și a răspunde automat (izolare, blocare). În contextul lanțului trofic, EDR ar trebui să fie instalat pe toate sistemele IT critice: servere care găzduiesc ERP, stații de lucru ale angajaților cu acces la date sensibile, chiar și pe anumite sisteme din fabrică care rulează Windows/Linux (de exemplu, HMI – Human Machine Interface – HMI – HMI Stations). Un EDR bine configurat poate prinde rapid ransomware-ul înainte ca acesta să se răspândească sau un atacator să încerce mișcări laterale. De exemplu, dacă un angajat face clic pe un fișier rău intenționat care primește un backdoor, EDR poate detecta execuția suspectă și poate **opri imediat procesul rău intenționat** , trimițând o alertă echipei de securitate.
- **Sisteme SIEM (Security Information and Event Management):** Un SIEM colectează și corelează jurnalele de evenimente din întreaga infrastructură – firewall, servere, controlere, aplicații – pentru a identifica potențialele incidente. În lanțul de aprovizionare cu alimente, un SIEM poate fi configurat pentru a monitoriza evenimente precum conexiuni neautorizate între rețeaua de producție și internet, eșecuri multiple de autentificare pe conturile de acces PLC, modificări neașteptate în fișierele de configurare HACCP etc. Prin corelarea acestor semne, SIEM poate genera **avertismente timpurii**. De exemplu, detectarea simultană a unui volum neobișnuit de trafic de date de la un server de baze de date și a unei conexiuni VPN deschise la ore neobișnuite ar putea indica exfiltrarea datelor – SIEM poate alerta și declanșa proceduri de răspuns. Implementarea SIEM este recomandată în special operatorilor mari, care dispun de resurse SOC (Security Operations Center) și pot analiza prompt alertele, dar IMM-urile pot recurge și la variante SIEM gestionate (MSSP).
- **Autentificare cu mai mulți factori (MFA) și management robust al accesului:** O măsură aparent simplă, MFA, s-a dovedit extrem de eficientă în prevenirea compromisurii conturilor chiar dacă parolele sunt furate. Orice acces la sisteme critice (VPN-uri la distanță, conturi de administrator, acces la platforme de gestionare a cloud-ului) trebuie să necesite doi sau mai mulți factori de autentificare (parolă + token hardware sau aplicație mobilă). Implementarea MFA ar fi putut preveni unele breșe mari (de exemplu, atacul JBS menționat mai sus, pornit de la acreditări furate reutilizate). În plus, principiul Zero **Trust** – "Nu aveți încredere în nimeni în mod implicit, verificați întotdeauna" – ar trebui adoptat ca politică generală. Aceasta înseamnă că fiecare solicitare de acces la un sistem, chiar și de la un angajat din rețea, este

tratată ca potențial neautorizată până când este verificată. Practic, Zero Trust se traduce în: segmentare (pe care am menționat-o deja), MFA peste tot, verificarea continuă a integrității dispozitivelor care se conectează (de exemplu, un computer cu antivirus dezactivat nu poate accesa serverele interne) și principiul privilegiului minim (fiecare cont sau aplicație are acces doar la resursele strict necesare).

- **Gestionarea actualizărilor și a corecțiilor:** Un număr semnificativ de incidente se bazează pe exploatarea vulnerabilităților cunoscute pentru care există deja patch-uri. De aceea, un program riguros de **gestionare a patch-urilor** este vital. Provocarea este majoră mai ales în zona OT: multe sisteme industriale nu acceptă opriri frecvente pentru actualizări sau folosesc echipamente care nu mai sunt suportate. Soluția presupune planificarea – patch-uri imediate pe sistemele IT (servere, PC-uri) și patch-uri programate pe ICS în ferestrele de mentenanță, eventual combinate cu măsuri compensatorii (izolare, monitorizare sporită) până la aplicarea patch-ului. De exemplu, dacă vulnerabilitatea critică afectează un PLC și nu poate fi remediată imediat, deoarece ar opri producția, compania poate implementa temporar o regulă de firewall care blochează accesul la porturile utilizate de acea vulnerabilitate și intensifică monitorizarea traficului către acel PLC până când acesta poate fi remediat în siguranță. **Actualizarea firmware-ului** la dispozitivele IoT din ferme sau depozite este din nou esențială, deoarece multe atacuri IoT se bazează pe versiuni vechi de firmware.
- **Backup-uri regulate și plan de recuperare în caz de dezastru:** Multe întreprinderi mici și-au dat seama de importanța backup-urilor doar după ce au suferit un atac ransomware. O bună practică este aplicarea regulii **3-2-1** : trei copii ale datelor, pe două medii diferite, una în afara amplasamentului (deconectată). Pentru producție, aceasta înseamnă să ai copii de rezervă atât pentru datele IT (baze de date de rețete, sisteme de contabilitate), cât și pentru configurațiile OT (programe PLC, configurații SCADA). Aceste copii de rezervă ar trebui testate periodic. Un plan de recuperare în caz de dezastru ar trebui să detalieze modul în care operațiunile sunt restabilite rapid în cazul unui incident major. De exemplu, dacă sistemul ERP al distribuitorului se defectează, care este procedura? (poate trecerea temporară la procesarea manuală a comenzilor, utilizarea fișierelor de rezervă etc.). Planul trebuie practicat, nu doar scris.
- **Monitorizare continuă și detectarea intruziunilor:** Pe lângă EDR și SIEM, care sunt soluții active, se recomandă utilizarea IDS/IPS (Sisteme de detectare/prevenire a intruziunilor) și pentru rețelele industriale. Există soluții specializate de monitorizare OT care pot detecta, de exemplu, comenzi neautorizate pe un protocol industrial (Modbus, OPC-UA) sau modificări neprogramate ale logicii unui PLC și pot alerta imediat. Unii pot chiar **bloca comanda suspectă** (IPS). Monitorizarea traficului de rețea în fabrică și zona depozitului (de exemplu, monitorizarea rețelelor de senzori wireless) poate dezvălui o activitate anormală (un dispozitiv nou care comunică ciudat, posibil un dispozitiv compromis). Investițiile în astfel de tehnologii sunt mai potrivite pentru întreprinderile mari, dar IMM-urile pot adopta și versiuni mai simple sau servicii de monitorizare externalizate.
- **Politici și proceduri de securitate (cadru organizațional):** Tehnologia nu poate acoperi totul fără reguli clare și respectate. Companiile trebuie să aibă politici scrise pentru securitatea parolelor (de exemplu, schimbarea periodică, complexitatea), utilizarea dispozitivelor mobile, accesul la date (cine și în ce condiții poate copia date sensibile). O **politică de control al accesului furnizorilor** este, de asemenea, crucială: de exemplu, ar trebui să existe proceduri pentru a acorda acces temporar unui tehnician de întreținere OT, astfel încât, după finalizarea lucrărilor, contul să fie dezactivat imediat. **Due diligence în onboarding furnizori** înseamnă evaluarea prealabilă a noilor parteneri din lanț: chestionare de securitate, audituri la fața locului sau solicitarea de certificări (ISO 27001 pentru furnizorii IT, de exemplu) înainte de conectarea acestora la sistemele interne. Contractele ar trebui să includă clauze de securitate cibernetică și notificare promptă în cazul unui incident (pentru a nu afla cu întârziere că un

furnizor a fost piratat). Un alt element este **gestionarea mediilor externe**: politica ar trebui să interzică utilizarea stick-urilor USB neautorizate în medii industriale și să prevadă scanarea oricărui echipament nou introdus (modelat după scanerele portabile despre care s-a vorbit în soluțiile TXOne – un dispozitiv pentru inspectarea noilor echipamente pentru malware înainte de conectare).

- **Formare și conștientizare (conștientizarea securității cibernetice):** Factorul uman rămâne adesea veriga slabă, dar poate deveni și cea mai puternică apărare dacă personalul este educat corespunzător. Toți angajații, de la lucrătorii din fabrică la managerii de top, ar trebui să urmeze cursuri regulate de conștientizare a securității cibernetice. Acestea trebuie adaptate contextului: lucrătorilor li se va explica de ce nu ar trebui să conecteze dispozitivele personale la rețeaua mașinilor și cum să recunoască un e-mail de phishing care pretinde că este de la un șef; Șoferilor de transport li se poate arăta cum să reacționeze dacă dispozitivul telematic din camion se comportă ciudat; Personal IT – politici de întărire și răspuns la incidente. O cultură puternică a securității înseamnă că angajații **raportează imediat** incidentele suspecte (un computer care "se luptă" după deschiderea unui fișier, un dispozitiv străin văzut în fabrică etc.), ceea ce permite echipei de răspuns să acționeze înainte ca daunele să escaladeze. Conducerea companiei trebuie să fie implicată în promovarea acestei culturi, astfel încât regulile de siguranță să fie respectate la fel de riguros ca și normele de siguranță alimentară.
- **Audituri de securitate și teste de penetrare:** Este dificil să știi cât de eficiente sunt implementate măsurile fără a le verifica practic. **Auditurile periodice** (interne sau terțe) pot evalua conformitatea cu politicile (de exemplu, un audit poate constata că, în ciuda politicii, unele servere critice nu au fost corectate timp de 6 luni). Mai amănunțit, **testele de penetrare** simulează atacuri reale pentru a găsi breșe. De exemplu, o echipă de pentesting angajată de un producător de băuturi ar putea încerca să pătrundă în rețeaua companiei prin diverse mijloace: phishing angajați, scanarea rețelei pentru porturi deschise, chiar acces fizic ascuns la sediu. Rezultatele acestor teste evidențiază **punctele slabe** înainte ca infractorii adevărați să le descopere. Se recomandă includerea componentelor OT în domeniul de testare, cu precauție (teste neintruzive, pentru a nu perturba producția). Un scenariu de testare util este un **exercițiu echipă roșie – echipă albastră în** care un grup simulează un atac complex asupra întregului lanț (inclusiv compromiterea unui furnizor fictiv), iar echipa de securitate internă trebuie să detecteze și să răspundă. Aceste exerciții dezvăluie atât vulnerabilități tehnice, cât și lacune în proceduri sau timpi de reacție.

Cele mai bune practici și recomandări personalizate (IMM-uri vs. companii mari)

Implementarea măsurilor de mai sus poate varia semnificativ în funcție de dimensiunea organizației și de resursele disponibile. Vom evidenția câteva recomandări distincte pentru **întreprinderile mici și mijlocii (IMM-uri)** din industria alimentară, respectiv pentru **marii operatori economici**:

- **IMM-uri (fabrici mici, ferme de procesare, depozite locale, magazine independente):** Acestea au adesea resurse IT limitate și nu au echipe de securitate dedicate. Cu toate acestea, nu sunt feriți de atacuri – infractorii le pot considera ținte mai ușoare. Bune practici pentru IMM-uri:
    - *Outsourcing și servicii gestionate:* Dacă nu își permit un departament de securitate IT, IMM-urile pot apela la **MSSP** (Managed Security Service Providers) sau consultanți pentru a-și configura și monitoriza securitatea de bază (firewall, antivirus, backup). Un MSSP poate furniza soluții EDR/SIEM pe bază de abonament, mai accesibile decât implementarea internă.
    - *Concentrați-vă pe elementele fundamentale:* Lucrul bun este că multe IMM-uri au infrastructuri mai simple. Prioritățile ar trebui să fie backup offline regulat pentru datele critice (în special rețete, formulare HACCP, date financiare), actualizări actualizate pentru toate PC-urile și sistemele (folosind actualizarea automată acolo

unde este posibil) și instruire minimă de conștientizare a personalului (să nu cadă în capcane evidente de phishing). De asemenea, utilizarea soluțiilor cloud pentru e-mail, stocare sau ERP (Software as a Service) poate transfera o parte din responsabilitatea de securitate către furnizori specializați (care au echipe de securitate). Desigur, trebuie făcute evaluări fiabile pentru acești furnizori.

- *Segregare simplă a rețelei:* Chiar și cu resurse limitate, lucruri precum router separat și rețea Wi-Fi separată pentru echipamente de producție vs. birou, schimbarea parolelor implicite pe toate dispozitivele (camere de supraveghere, routere etc.), dezactivarea serviciilor neutilizate poate fi realizată. Aceste acțiuni nu costă mult, dar reduc vectorii de atac.
- *Plan simplificat de răspuns la incidente:* IMM-urile ar trebui să aibă cel puțin un **plan de răspuns în caz de** atac cibernetic: cine este chemat (furnizor IT, poliție, CERT național?), cum să izoleze rapid sistemele infectate (cine scoate cablul de pe server), cum să comunice intern și extern (să anunțe clienții dacă este cazul). Repetarea acestui plan o dată pe an (cel puțin pe hârtie) va ajuta enorm în cazul real.

- **Companii mari (grupuri alimentare, lanțuri de retail, procesatori cu zeci de fabrici):** Aceste organizații au infrastructuri extinse și sunt ținte atractive pentru atacuri sofisticate. Bună practică pentru ei:
  - *Alinierea la standarde și cadre recunoscute:* Este recomandabil ca companiile mari să implementeze un **ISMS (Information Security Management System)** conform ISO 27001, care include evaluări periodice ale riscurilor (conform ISO 27005) și controale documentate. De asemenea, standarde specifice, cum ar fi **ISA 62443** pentru medii industriale, pot ghida practicile de securitate OT. Respectarea unor astfel de standarde oferă un **cadru holistic** și poate îmbunătăți, de asemenea, imaginea companiei în fața partenerilor (demonstrează maturitate în ceea ce privește securitatea).
  - *Investiții în tehnologii avansate:* Pe lângă EDR și SIEM, companiile mari pot adopta soluții precum **monitorizarea industrială avansată** (de exemplu, platforme de securitate OT care mapează toate activele din fabrici și detectează anomalii în trafic), **analiza comportamentului utilizatorilor** (UEBA – User and Entity Behavior Analytics, care ar detecta activitățile anormale ale unui cont legitim) sau chiar inteligența artificială pentru detectarea amenințărilor. De asemenea, pot implementa sisteme redundante și centrate pe disponibilitate (de exemplu, centre de date de rezervă sincronizate, în cazul în care unul este atacat, celălalt preia rapid controlul).
  - *Echipe și parteneriate dedicate:* Operatorii mari ar trebui să aibă o echipă internă **CSIRT** (Computer Security Incident Response Team) sau o echipă albastră care monitorizează și răspunde la incidente 24/7. Colaborarea cu organisme specializate este, de asemenea, utilă: de exemplu, în sectorul alimentar global există Food and Ag-ISAC (centrul de schimb de informații despre amenințări) care oferă alerte despre atacurile emergente. Companiile mari ar trebui să fie membri activi ai unor astfel de inițiative pentru a fi conștienți de noile tactici folosite de atacatori.
  - *Testare complexă și evaluare continuă:* O companie mare își poate permite și ar trebui să execute periodic **exerciții de gestionare a crizelor** care simulează atacuri majore. Implicarea conducerii de top în **exercițiile de masă** va asigura că, în cazul unui incident real, deciziile (de exemplu, oprirea temporară a producției, efectuarea de notificări publice sau plata/neplata unei răscumpărări) sunt luate rapid și în cunoștință de cauză. Un exemplu de bună practică este organizarea de exerciții de formare naționale sau sectoriale – în 2024 CISA (agenția americană de securitate cibernetică) a desfășurat **exercițiul Cyber Storm** axat pe sectorul alimentar și agricol, reunind companii mari pentru a-și testa coordonarea și răspunsul la atacuri simulate.

Participarea la astfel de exerciții (sau replicarea lor internă) pregătește organizațiile pentru situații din lumea reală.

Concluzii finale

Securitatea cibernetică a lanțului de aprovizionare în sectorul alimentar nu mai poate fi ignorată – incidentele recente au arătat că, de la ferme la supermarketuri, fiecare componentă poate fi perturbată de atacuri digitale, cu consecințe asupra alimentelor pentru populație, încrederea consumatorilor și stabilitatea economică. O abordare proactivă, care combină **practica tehnică** (implementarea controalelor și tehnologiilor adecvate), **povestirea narativă** (înțelegerea posibilelor scenarii de atac și pregătirea pentru ele) și **rigoarea academică** (alinierea la standarde și metodologii recunoscute, bazate pe studii și rapoarte) este necesară pentru a asigura reziliența acestui sector critic. În esență, companiile trebuie să construiască un mediu în care riscurile să fie cunoscute și ținute sub control, în care un potențial incident cibernetic să poată fi izolat rapid fără a dăuna consumatorului final. Prin punerea în aplicare a măsurilor discutate și cultivarea unei culturi a securității, sectorul agroalimentar își poate proteja **lanțul de aprovizionare** împotriva amenințărilor cibernetice din ce în ce mai sofisticate, asigurând în același timp siguranța alimentară și continuitatea aprovizionării.

Continuitate operațională

Continuitatea afacerii se referă la capacitatea unei organizații de a-și menține funcțiile esențiale în timpul și după un incident major (fie el cibernetic, tehnologic sau chiar fizic, cum ar fi un dezastru natural). În contextul lanțului de aprovizionare cu alimente, **planificarea continuității** este crucială, deoarece perturbările pot avea consecințe imediate asupra aprovizionării populației. Directivele NIS2 și legislația națională subliniază importanța acestui lucru: entitățile trebuie să ia **măsuri pentru a asigura continuitatea serviciilor esențiale** în caz de perturbare cibernetică. Acest capitol analizează modul de pregătire pentru astfel de situații și instrumentele de planificare disponibile.

Planificarea continuității

Primul pas în asigurarea continuității este efectuarea unei analize a impactului asupra afacerii (BIA). Prin BIA, compania identifică ce procese și activități sunt critice, care sunt dependențele, dependențele etc. De exemplu, un procesator de lapte poate determina că oprirea liniei pasteurizate duce la deteriorarea materiei prime, de unde și RTO pentru sistemul de control al pasteurizării; de asemenea, pierderea datelor de trasabilitate pentru mai mult de ultima oră de producție (RPO = 1 oră) ar compromite capacitatea de a face rechemări precise, astfel încât backup-urile datelor trebuie făcute cel puțin o dată la oră.

Odată ce cerințele de recuperare au fost identificate, pot fi dezvoltate **strategii de continuitate** . Acestea includ: redundanța infrastructurii (sisteme duplicate sau servere de rezervă), stocuri de siguranță (de materii prime sau produse finite) pentru acoperirea întârzierilor, diversificarea furnizorilor (pentru a avea o alternativă în cazul în care cea principală nu este disponibilă), planuri de relocare temporară a producției (dacă o fabrică se defectează, alta poate prelua parțial comenzi), proceduri manuale de lucru (de exemplu, emiterea de facturi manuale dacă sistemul informatic este oprit), etc. Un accent deosebit este pus pe **backup-ul și recuperarea datelor**: toate datele critice (rețete, comenzi, configurații de echipamente) trebuie copiate periodic și stocate în siguranță, testându-le recuperarea. Multe incidente cibernetice (cum ar fi ransomware-ul) pot fi depășite mai repede dacă există copii de rezervă valide și un plan de recuperare rapidă.

Planul de continuitate a afacerii (BCP)

Instrumentul central este dezvoltarea unui plan de **continuitate a activității (BCP).** Acesta este un document cuprinzător care descrie *modul în care* funcțiile critice vor fi menținute sau restaurate în cazul unui dezastru sau incident major. Pentru organizațiile NIS (esențiale/importante), existența unui

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

PCF actualizat și testat este o necesitate practică și, implicit, așteptată de autorități ca parte a măsurilor de securitate. Un PCF specific pentru lanțul alimentar va conține:

- **Scop și domeniu de aplicare:** ce scenarii acoperă (de exemplu, atac cibernetic sever, întrerupere prelungită a curentului, indisponibilitatea unui furnizor cheie, pandemie etc.) și ce unități ale organizației sunt implicate.
- **Echipa de criză și responsabilități:** o listă nominală a membrilor *echipei de continuitate/management al crizei*, cu rolurile fiecăruia (lider de echipă, comunicare, IT, producție, logistică, serviciu clienți etc.) și date de contact de urgență (telefon alternativ, e-mail personal în cazul în care rețeaua corporativă este oprită etc.). De exemplu, directorul de operațiuni poate fi șeful comitetului de criză, CIO responsabil cu restaurarea IT, managerul de producție pentru reluarea producției etc.
- **Proceduri de răspuns imediat:** măsurile care trebuie luate imediat după detectarea unui incident grav. Acestea pot include *planuri scurte de acțiune (playbook),* cum ar fi în cazul ransomware-ului – deconectarea sistemelor afectate de la rețea, pornirea serverelor de rezervă dacă există, anunțarea echipei de securitate; în cazul unei căderi a sistemului SCADA – punerea instalațiilor sub control manual conform procedurii X, informarea supraveghetorilor de tură etc. Aceste acțiuni imediate au rolul de a limita impactul și de a pregăti terenul pentru redresare.
- **Planuri de continuitate pentru fiecare funcție critică:** detalierea modului în care va fi menținut fiecare proces critic identificat (prin BIA). De exemplu, planul de continuitate pentru **procesarea comenzilor**: dacă platforma IT de primire a comenzilor online nu funcționează, comenzile vor fi primite prin telefon/fax la un număr de rezervă, personalul de vânzări va fi realocat pentru a le prelua manual, acestea vor fi notate într-un registru și apoi introduse în sistem la revenire. Un alt exemplu este un plan de continuitate a producției: dacă fabrica principală este nefuncțională timp de 24 de ore, livrarea din stocurile existente va fi prioritară, producția va fi subcontractată temporar unui partener (dacă există un acord) sau va fi livrată dintr-o altă locație. Aceste planuri trebuie să fie cât mai concrete și operaționale posibil.
- **Resurse necesare și logistice:** ce resurse sunt critice și cum sunt furnizate în caz de incident – de la alimentarea cu energie electrică de urgență (generatoare pentru depozitare frigorifică, de exemplu), la acces de rezervă la internet, la vehicule de transport alternative. Dacă, de exemplu, sistemul de rutare a camioanelor eșuează, șoferii trebuie să aibă o procedură de comunicare (prin telefon, SMS) pentru a primi instrucțiuni de livrare.
- **Comunicare în caz de criză:** planul trebuie să includă mesaje și canale de comunicare predefinite atât *interne* (pentru angajați: ce să facă, unde să se prezinte, cum să continue activitatea), cât și *externe* (către clienți, furnizori, autorități, mass-media). În lanțul alimentar, comunicarea promptă cu comercianții cu amănuntul sau distribuitorii este esențială dacă livrările sunt întârziate. De asemenea, în cazul în care există riscul ca produsele nesigure să ajungă pe piață, trebuie pregătită comunicarea privind rechemarea și informarea publică, în coordonare cu autoritățile sanitare.
- **Proceduri de recuperare în caz de dezastru (IT):** deși uneori este un plan separat (DRP – Disaster Recovery Plan), BCP include măsuri concrete pentru restabilirea infrastructurii IT și reluarea operațiunilor normale. Aceasta include: secvența de restaurare a serverelor din backup, reconectarea rețelelor, verificarea integrității datelor recuperate, testarea aplicațiilor critice etc., în ordinea stabilită de prioritățile afacerii. De exemplu, se stabilește că ERP

(sistemul de planificare a resurselor întreprinderii) trebuie restabilit în 8 ore, site-ul public poate aștepta 48 de ore și așa mai departe.

- **Planuri de suspendare:** odată ce criza a trecut și sistemele sunt restabilite, planul trebuie să acopere modul de tranziție de la procedurile provizorii la cele normale, restabilirea controalelor standard, evaluarea stării activității (de exemplu, inventarul întârzierilor, întârzierile la livrare, reluarea producției la capacitate maximă). Aici intervin și **lecțiile învățate**: organizarea unui debriefing post-incident și actualizarea planurilor pe baza a ceea ce se găsește.

Un **scurt plan de continuitate** (sau *o versiune sumară*) este adesea folosit ca ghid practic pentru situații de criză – un document condensat, de câteva pagini sau chiar un afiș, care conține informațiile esențiale: contacte de urgență, pași imediați de urmat, priorități de redresare. Este ușor accesibil și ușor de înțeles pentru toți angajații cheie, servind ca o listă *de verificare* în perioadele de tensiune ridicată. De exemplu, o **listă de verificare a acțiunilor în cazul unui incident major** poate arăta astfel: 1) Asigurați-vă că personalul este în siguranță; 2) Confirmă natura incidentului (cibernetic, IT, fizic); 3) Informează managerul X și echipa de criză; 4) Activarea planului de continuitate – consultați secțiunea relevantă (IT/producție); 5) Comunică intern "modul de urgență" activat; etc.

Pe de altă parte, **planul complet de continuitate** este documentul detaliat pe care l-am descris mai sus, care oferă toate informațiile necesare pentru a gestiona criza pas cu pas. Este bine ca organizațiile să aibă ambele versiuni: planul complet, actualizat anual sau ori de câte ori apar modificări (de exemplu, sisteme noi, reorganizări) și declarații operaționale (scurte) pentru utilizare rapidă.

Un aspect critic este **testarea și actualizarea planurilor**. Un plan de continuitate este valoros numai dacă a fost testat în prealabil, altfel pot exista lacune nedetectate. Testarea poate fi de mai multe feluri: *exerciții de verificare a biroului* (revizuirea teoretică a planului de echipă), *exerciții de simulare* (de exemplu, simulezi că sistemul ERP nu este disponibil și vezi cum reacționează echipa timp de câteva ore lucrând după proceduri alternative), *teste tehnice de failover* (pornirea serverelor de backup, rularea sistemelor pe generator etc.). ENISA și bunele practici recomandă planurile de testare **cel puțin o dată pe an** și ori de câte ori apar schimbări majore în organizație.

În România și Bulgaria, companiile din sectorul alimentar esențial/important vor trebui să includă planuri de continuitate în măsurile lor generale de securitate. Autoritățile pot solicita înregistrări ale testelor efectuate sau pot organiza exerciții sectoriale. De exemplu, ne putem aștepta ca DNSC (RO) sau echivalentul în BG să inițieze **exerciții de criză cibernetică** în sectorul alimentar, similare celor organizate în sectoare precum energie sau finanțe, pentru a verifica nivelul de pregătire.

În concluzie, continuitatea operațională este *plasa de siguranță a* lanțului de aprovizionare. Oricât de robuste sunt măsurile de prevenire, un incident grav poate apărea, iar diferența dintre un impact minor și un dezastru va fi făcută de gradul de pregătire și capacitatea de a reacționa rapid. Companiile care au planuri bine dezvoltate vor putea depăși incidentele, protejându-și atât afacerea, cât și consumatorii. Ceilalți riscă nu doar sancțiuni legale, ci și pierderea ireparabilă a încrederii în piață. Continuitatea trebuie văzută ca o investiție indispensabilă în **reziliența** lanțului alimentar.

Răspuns la incidente

Chiar și cu un management robust al riscurilor și măsuri preventive robuste, niciun sistem nu este infailibil. Prin urmare, capacitatea de a **răspunde eficient la incidentele cibernetice** este o componentă critică a strategiei de securitate. Răspunsul la incidente constă într-un set de procese și proceduri prin care o organizație detectează, investighează, limitează și recuperează în urma incidentelor de securitate, minimizând impactul acestora. Directiva NIS2 impune entităților esențiale și importante nu numai să prevină, ci și să **gestioneze incidentele într-o manieră profesionistă**, inclusiv prin notificarea autorităților competente într-un interval de timp strict. Acest capitol

abordează modul de organizare a răspunsului la incidentele din lanțul de aprovizionare cu alimente, atât intern în cadrul companiilor, cât și în interacțiune cu autoritățile și partenerii.

Organizarea echipei de răspuns la incidente (CSIRT intern)

Primul pas este înființarea unei echipe **de răspuns la incidente** în cadrul organizației. Acest lucru este adesea denumit CSIRT (Computer Security Incident Response Team) sau IRT. În companiile mai mici, poate fi un grup ad-hoc de angajați cu abilități IT, sub coordonarea managerului IT sau a responsabilului de securitate. În companiile mari, există echipe de securitate dedicate (SOCs – Security Operations Center) care monitorizează și reacționează continuu la alerte. Indiferent de dimensiune, este important ca rolurile să fie bine definite: cine analizează alertele, cine decide să escaladeze un incident major, cine comunică extern etc. Un **plan de răspuns la incidente (IRP)** documentează aceste aspecte, similar cu modul în care BCP documentează continuitatea.

Pașii standard ai ciclului de răspuns la incidente, conform NIST și altor bune practici, sunt **pregătirea, detectarea și analiza, izolarea și eradicarea, recuperarea, lecțiile învățate**.

- **Pregătire:** include toate activitățile preliminare care asigură că echipa este pregătită să intervină. Aceasta include definirea politicilor de incidente (ce tipuri de evenimente constituie un "incident" și cât de grave pot fi), implementarea sistemelor de detecție (monitorizarea rețelei, sisteme IDS/IPS, alarme pe servere), pregătirea instrumentelor de investigație (software de analiză malware, acces la jurnale centralizate), precum și instruirea echipei. În sectorul alimentar, instruirea trebuie să țină cont de specificul ICS: echipa de răspuns trebuie să includă sau să poată apela la ingineri de automatizare care cunosc sistemele industriale, nu doar experți IT, deoarece analiza unui incident pe un PLC sau SCADA necesită cunoștințe OT.

- **Detectare și analiză:** momentul în care apare și este identificat un eveniment suspect. Sursele pot fi automate (un sistem de monitorizare detectează traficul anormal, un endpoint antivirus alertează despre malware, un indicator de compromitere primit de la CERT arată prezența în sisteme) sau umane (un angajat raportează un comportament ciudat al PC-ului, un partener anunță că a fost atacat și poate că s-au propagat probleme). Analiza inițială determină dacă este un *incident real*, ce tip (exfiltrare de date, ransomware, DoS, compromitere a contului etc.), ce sisteme sunt afectate și estimează impactul. Această fază este crucială și dificilă – statistic, multe organizații descoperă incursiuni târziu (pot trece zile sau săptămâni între compromitere și detectare). De aceea, practici precum *vânătoarea proactivă a amenințărilor* sau supravegherea atentă a jurnalelor sunt valoroase. În lanțul trofic, un semn de alarmă ar putea fi un server PLC care repornește neprogramat, o creștere nejustificată a traficului între rețelele de birou și industriale, un cont de utilizator care lansează comenzi neobișnuite la momente nepotrivite etc.

- **Limitare, eradicare:** Odată ce un incident este confirmat, prioritatea imediată este **limitarea daunelor**. Acest lucru poate însemna izolarea segmentului afectat (deconectarea unei rețele, închiderea unui server compromis), blocarea accesului atacatorului (schimbarea parolelor, blocarea conturilor suspecte) și prevenirea răspândirii acestuia (de exemplu, dacă este detectat malware pe un PC, PC-ul este deconectat și orice altceva este verificat). În cazul ransomware-ului de criptare a fișierelor, izolarea înseamnă oprirea răspândirii în rețea cât mai repede posibil – ceea ce implică uneori decizia dificilă de a opri temporar anumite sisteme critice în mod preventiv. În paralel, **începe eradicarea cauzei**: identificarea și eliminarea malware-ului, închiderea vulnerabilităților exploatate (de exemplu, aplicarea unui patch dacă a fost introdusă o vulnerabilitate cunoscută), eliminarea persistenței (backdoor-uri lăsate de

atacator). Această etapă trebuie făcută cu atenție: dacă acționați prea încet, atacatorul poate provoca mai multe daune; Dacă se iau măsuri prea repede sau nepregătite, se pot pierde dovezi importante pentru investigație. Uneori sunt folosite companii specializate în răspunsul la incidente, în special pentru incidente grave – în România și Bulgaria există astfel de servicii, fie furnizate de echipe interne de integratori, fie de echipe internaționale care pot interveni la cerere.

- **Recuperare:** Odată ce amenințarea imediată este neutralizată, accentul se mută pe recuperarea sistemelor și revenirea la operațiuni normale și sigure. Dacă un server a fost afectat, acesta se poate reconstrui din backup și se poate reintegra în rețea doar după ce suntem siguri că nu va fi reinfectat. În cazul furtului de date, recuperarea înseamnă și restabilirea integrității datelor și gestionarea consecințelor (de exemplu, resetarea acreditărilor compromise). Planul de Continuitate (BCP) discutat mai devreme este strâns legat de această fază: dacă a fost activat, trecerea de la sistemele temporare la cele restaurate se face acum. Un aspect aparte: în industria alimentară, dacă incidentul a afectat procesele de producție, recuperarea presupune verificări de calitate. De exemplu, dacă liniile de producție s-au oprit brusc, la repornire trebuie testat dacă parametrii de calitate se încadrează în parametri, iar produsul final este sigur (conform standardelor alimentare). Prin urmare, echipa de calitate și conformitate alimentară este implicată alături de echipa IT în validarea revenirii la normal.

- **Post-incident/lecții învățate:** Ultimul pas formal este analizarea incidentului după rezolvare, pentru a documenta ce s-a întâmplat, cum a fost răspuns și ce poate fi îmbunătățit. Se **întocmește un raport detaliat al** incidentelor, care include cronologia, vectorul de atac, impactul (active afectate, timp de nefuncționare, pierderi), măsurile luate și recomandările. Acest raport este util intern (pentru a preveni viitoare incidente similare), dar și extern – este practic informația care va sta la baza notificării finale către autoritatea competentă, conform NIS2 (raportul care trebuie trimis la 1 lună de la incident). De asemenea, această analiză post-mortem poate dezvălui nevoi de investiții sau de schimbare a politicii (de exemplu, dacă incidentul a fost posibil din cauza lipsei unui management riguros al patch-urilor, abordarea acestui decalaj va fi prioritară).

Notificarea incidentelor și cooperarea cu autoritățile

Conform Directivei NIS2 (și legislațiilor naționale asociate, cum ar fi OUG 155/2024 în RO), companiile din lanțul alimentar clasificate ca entități importante trebuie să **notifice autoritățile** (DNSC din România, viitoarea autoritate desemnată din Bulgaria - autoritatea națională competentă și CERT-BG) atunci când suferă un incident cu impact semnificativ. Definiția unui "incident semnificativ" ia în considerare mai mulți factori: numărul de beneficiari afectați, durata, domeniul geografic de aplicare, gravitatea întreruperii serviciului, impactul economic sau societal. Un atac care oprește producția pentru câteva ore poate fi nesemnificativ, dar unul care face imposibilă livrarea alimentelor într-o zi într-o regiune largă ar fi considerat semnificativ și, prin urmare, notificabil.

Mecanismul de raportare a fost detaliat anterior: în mod ideal o alertă inițială în termen de 24 de ore, notificare completă în termen de 72 de ore și raport final după 30 de zile. În practică, companiile trebuie să stabilească *un protocol intern*: cine are autoritatea de a notifica (de obicei șeful NIS sau CISO, cu aprobarea conducerii), ce informații sunt trimise și cum. Pentru a facilita acest lucru, se recomandă pregătirea unui **formular de notificare a incidentului** (sau șablon) care să conțină câmpurile necesare. Un exemplu de formular de **notificare a incidentului** ar include:

- **Detalii despre entitatea raportoare:** numele organizației, persoana de contact (ofițer NIS), date de contact (telefon, e-mail).

- **Tipul de entitate și sector: Entitate** majoră, sectorul alimentar (producție/procesare/distribuție).
- **Data și ora detectării incidentului:** ... (precizie oră/minut).
- **Scurtă descriere a incidentului:** de exemplu "Atac ransomware care a afectat serverele de producție și sistemele de gestionare a stocurilor".
- **Impactul inițial evaluat:** sisteme afectate (de exemplu: "SCADA la fabrica X, ERP indisponibil"), servicii întrerupte ("producție oprită timp de 8 ore, livrări întârziate"), ponderea estimată a daunelor (de exemplu: "~30% din volumul zilnic de producție întârziat").
- **Cauza potențială:** dacă este cunoscută sau suspectată – de exemplu: "suspiciunea unui atac cibernetic de phishing (ransomware); fișiere criptate și note de răscumpărare observate."
- **Măsuri luate imediat:** de exemplu: "Segmentarea rețelei, sisteme infectate izolate, plan de continuitate activat – livrări onorate din stocuri".
- **Posibil impact transfrontalier:** de exemplu, "Da, livrările către doi parteneri dintr-un alt stat membru (Bulgaria) pot fi întârziate" sau "Nu, impact localizat".
- **Nevoia de asistență:** opțional, dacă compania solicită asistență din partea autorităților/CSIRT.
- **Alte informații relevante:** orice detalii tehnice (indicatori cunoscuți de compromitere, IP-uri de atac) sau context.

Acest formular ar corespunde notificării inițiale/în termen de 72 de ore. Ulterior, raportul final va conține analiza completă: vectorul confirmat, vulnerabilitățile exploatate, volumul exact al impactului (ex: "12.000 de tone de producție întârziată, recuperată ulterior", "nu s-a detectat exfiltrarea datelor" etc.), precum și măsurile corective implementate (patch-uri aplicate, practici modificate). Scopul notificării nu este de a sancționa entitatea raportoare pentru că a suferit un atac (victimizarea nu este vină), ci de a permite autorităților să monitorizeze amenințările și, dacă este necesar, să alerteze alți operatori sau să ofere sprijin. Totodată, **cooperarea cu autoritățile** presupune că, dacă este necesar, compania va furniza informații suplimentare, va permite investigații (indiferent dacă atacul este de interes național sau criminal) și va implementa recomandările primite.

În România, DNSC centralizează notificările. Este posibil ca DNSC să ofere o platformă de raportare online sau adrese dedicate. În Bulgaria, CERT Bulgaria va juca un rol similar. De menționat că legislația NIS2 interzice utilizarea informațiilor obținute prin notificări pentru a incrimina entitatea raportoare – deci scopul este cooperarea, nu învinuirea victimei.

Cele mai bune practici europene în gestionarea riscurilor și securitatea lanțului de aprovizionare

Pentru a sprijini entitățile în implementarea cerințelor NIS2 și creșterea nivelului de securitate, instituțiile europene și organismele de standardizare au elaborat o serie de **standarde, ghiduri și bune practici relevante**. Adoptarea acestor criterii de referință comune facilitează un nivel uniform de protecție și asigură interoperabilitatea măsurilor de securitate între lanțurile transfrontaliere. Mai jos, sintetizăm cele mai importante surse de bune practici la nivel european și internațional aplicabile managementului riscurilor în lanțul de aprovizionare cu alimente:

- **Standarde internaționale ISO/IEC:** Familia de standarde ISO 27000 oferă un cadru general pentru securitatea informațiilor (ISO/IEC 27001 stabilește cerințele pentru un sistem de management al securității informațiilor – ISMS, iar ISO/IEC 27002 oferă îndrumări pentru implementarea controalelor). Aceste standarde includ cerințe legate de evaluarea riscurilor și tratarea riscurilor la furnizori. De interes deosebit este **seria ISO/IEC 27036 – Managementul securității în relațiile de aprovizionare**: această serie acoperă etapele

relației cu furnizorii (planificare, selecție, contractare, management, reziliere) din perspectivă de securitate. Prin adoptarea ISO 27036, o organizație își structurează programul de securitate a lanțului de aprovizionare, având politici și controale pentru fiecare fază (de exemplu: impunerea cerințelor de securitate în contracte, evaluări periodice ale furnizorilor, proceduri securizate de off-boarding la încetarea colaborării). De asemenea, **standardul ISO 28000** (managementul securității pentru lanțul de aprovizionare) oferă un cadru general pentru managementul riscurilor în lanțurile de aprovizionare, deși are o perspectivă mai largă (inclusiv riscurile fizice) și nu abordează în mod specific securitatea cibernetică. Pentru sectorul alimentar, combinația dintre ISO 22000 (siguranța alimentară) și ISO 27001/27036 (securitatea informațiilor) poate oferi un sistem integrat de management al riscurilor de toate tipurile.

- **Orientările ENISA:** Agenția UE pentru Securitate Cibernetică (ENISA) are un rol activ în diseminarea bunelor practici. Raportul **"Bune practici pentru securitatea cibernetică a lanțului de aprovizionare" (ENISA, 2023)** este o referință esențială. Acesta prezintă concluziile unui studiu privind practicile actuale din entitățile-cheie și importante din UE și face recomandări cu privire la cinci domenii: abordarea strategică, managementul riscului lanțului, managementul relațiilor cu furnizorii, managementul vulnerabilităților, asigurarea calității produselor și practicile de securitate la furnizori. Unele bune practici concrete evidențiate de ENISA includ: *integrarea riscurilor lanțului în guvernanța corporativă* (asumarea responsabilității la nivelul conducerii superioare și alocarea de resurse dedicate), *menținerea unui inventar actualizat al tuturor furnizorilor și serviciilor externalizate*, *clasificarea furnizorilor în funcție de categoriile de risc* (critice, medii, scăzute) și aplicarea unor controale proporționale pentru fiecare categorie; *includerea cerințelor de securitate în procesele de achiziții* publice (de la RFP la clauze contractuale specifice), *monitorizarea continuă a performanței de securitate a furnizorilor critici* (eventual prin servicii de rating de securitate sau audituri independente), precum și *stabilirea de canale de comunicare pentru incidentele de securitate cu furnizorii*. ENISA recomandă, de asemenea, adoptarea unei *abordări colaborative*: în loc să impună unilateral cerințe furnizorilor mici, companiile mai mari le pot oferi asistență și know-how pentru a-și îmbunătăți securitatea (model de relație de "mentorat" în lanț).

- **Cadrul NIST pentru managementul riscului lanțului de aprovizionare (Cyber SCRM):** Deși își are originea în SUA, NIST SP 800-161 (revizuirea 1, 2022) a devenit un punct de referință internațional în practică. Acesta propune un model de management al riscului pe mai multe niveluri în lanț, aliniat cu controalele NIST SP 800-53. Multe companii multinaționale, inclusiv din Europa, sunt inspirate de NIST pentru a crea programe riguroase SCRM (Supply Chain Risk Management). Câteva principii NIST: implicarea tuturor funcțiilor relevante (nu numai IT, ci și departamentul de achiziții, juridic, financiar etc. în evaluarea riscurilor furnizorilor), evaluarea **riscurilor de reziliență cibernetică** și **operațională** (de exemplu, capacitatea furnizorului de a livra în caz de întreruperi), cerința ca furnizorii critici să aibă și practici de securitate solide și planuri de continuitate, și abordarea lanțului ciclului de viață (de la proiectare – asigurarea achiziționării de echipamente/software securizate – până la casare – asigurarea distrugerii în siguranță a datelor și dispozitivelor).

- **Practicile agențiilor naționale (BSI, ANSSI etc.):** Organismele naționale din țările din Europa de Vest au publicat ghiduri care pot servi drept model. De exemplu, **BSI (Germania)** are o serie de recomandări privind *evaluarea furnizorilor de cloud* și *cerințele minime de securitate în contracte*, care pot fi adaptate și pentru alți furnizori. **ANSSI (Franța)**

promovează metodologia **EBIOS Risk Manager**, utilizată de multe organizații franceze pentru analiza riscurilor, care include identificarea *părților interesate externe* și a riscurilor care decurg din relațiile acestora. ANSSI a emis, de asemenea, orientări sectoriale de securitate, iar unele principii (de exemplu, necesitatea autentificării puternice și a conectării în sistemele industriale) sunt universal aplicabile. **CERT-UK** (înainte de Brexit) a dezvoltat un set de 10 pași pentru a securiza lanțul de aprovizionare, punând accentul pe *due diligence* și pe evaluările anuale ale riscurilor. Prin intermediul rețelelor de cooperare, aceste cunoștințe au fost răspândite: ENISA compilează astfel de bune practici naționale în rapoartele sale.

- **Certificarea securității cibernetice și asigurarea calității:** Sistemele voluntare de certificare a securității (cadrul UE de certificare a securității cibernetice, în conformitate cu Legea privind securitatea cibernetică) sunt în curs de elaborare la nivelul UE. De exemplu, există o schemă de certificare pentru serviciile cloud (EUCS), care include cerințele lanțului de aprovizionare. În viitor, achiziționarea de produse și servicii certificate la nivelul UE va deveni o bună practică – companiile din lanțul alimentar vor putea alege furnizori cu certificări de securitate recunoscute. În plus, **este avută în vedere Legea privind reziliența cibernetică**, care va impune producătorilor de produse digitale (inclusiv echipamente IoT industriale) să respecte cerințele minime de securitate și să ofere asistență (patch-uri) pe toată durata de viață a produsului. Această inițiativă va crește calitatea generală a echipamentelor utilizate în industrie, reducând riscurile în lanț cauzate de produse vulnerabile sau nesecurizate.

- **Cultura securității și factorul uman:** O bună practică generală, dar care merită subliniată, este *investiția în conștientizare și instruire*. Agenția Uniunii Europene ENISA subliniază că organizațiile ar trebui să deruleze programe de formare personalizate pentru diferite categorii de personal – de la management (pentru a înțelege riscurile la nivel de business, conform cerințelor NIS2 privind responsabilitatea managementului) până la angajații operaționali (pentru a recunoaște tentativele de phishing și a respecta procedurile de securitate). Studiile arată că *eroarea umană rămâne principala cauză a incidentelor*, astfel încât nicio măsură tehnică nu acoperă nevoia unei culturi de securitate robuste. Companiile avansate au creat programe *de "igienă cibernetică"* cu verificări periodice (de exemplu, simulări de phishing trimise intern pentru instruire, premii pentru echipele cu cele mai puține greșeli, afișe și memento-uri în fabrici cu privire la regulile de conectare etc.).

- **Colaborarea și schimbul de informații de informații:** La nivel european există platforme pentru schimbul de indicatori (Threat Intelligence), cum ar fi instanțele MISP la care participă și entități private. O bună practică este alăturarea unor astfel de comunități – de exemplu, în România, centrul DNSC facilitează schimbul de alerte cu companiile prin canale precum Traffic Light Protocol (TLP) sau prin platforme precum RO-CSIRT. În Bulgaria, CSIRT facilitează schimbul de alerte cu companiile prin canale precum Traffic Light Protocol (TLP). În cadrul Direcției pentru Securitatea Rețelelor și a Informațiilor din cadrul Ministerului Guvernării Electronice, a fost înființat un Centru de Analiză și Schimb de Informații (ISAC). Acest centru joacă un rol crucial în:

    - Analiza amenințărilor cibernetice la nivel național;
    - Partajarea indicatorilor de compromis (IoC) cu celelalte autorități cheie de securitate cibernetică;
    - Sprijinirea coordonării naționale privind informațiile privind amenințările cibernetice.
    - Schimbul de informații se realizează în conformitate cu Traffic Light Protocol (TLP) pentru a asigura manipularea și diseminarea adecvată a datelor sensibile. Centrul

gestionează, de asemenea, informații clasificate, inclusiv materiale clasificate NATO și UE, în conformitate cu reglementările și protocoalele de securitate aplicabile.

- În plus, Direcția operează un Centru de Operațiuni de Securitate (SOC) responsabil cu monitorizarea activităților cibernetice rău intenționate și propune includerea IoC-urilor relevante în listele de blocare menținute intern de fiecare instituție.
- În cadrul acestei direcții se află și CERT (Computer Emergency Response Team). Colaborează cu părțile interesate interne și internaționale pentru a răspunde la incidente și pentru a împărtăși informații critice despre amenințări. CERT operează o instanță MISP (Malware Information Sharing Platform) pentru a facilita schimbul structurat de date despre amenințări cu partenerii și pentru a sprijini eforturile proactive de securitate cibernetică.

Companiile mari pot utiliza, de asemenea, serviciile comerciale de informații cibernetice pentru a fi alertate dacă, de exemplu, forumurile hackerilor discută despre vizarea sectorului alimentar sau apar exploit-uri zero-day care le-ar putea afecta infrastructura.

Pe scurt, bunele practici europene necesită o **abordare holistică**: combinarea standardelor internaționale cu orientările agențiilor, adaptarea acestora la propriul context și participarea activă la ecosistemul de securitate (prin certificare, schimb de informații, cooperare). Entitățile din lanțul de aprovizionare cu alimente din România și Bulgaria ar trebui să aspire la implementarea unui **cadru de securitate cibernetică** echivalent cu cel al companiilor din statele vest-europene. NIS2 stabilește un minim obligatoriu, dar în practică companiile pot și ar trebui să meargă dincolo de el – fiecare măsură proactivă (fie că este vorba de auditarea suplimentară a furnizorilor sau de dublarea pregătirii tehnicienilor de întreținere) poate preveni un incident costisitor. Iar alinierea la standarde recunoscute (ISO, NIST etc.) are și beneficii de business: facilitează demonstrarea conformității, câștigă încrederea partenerilor și poate fi un avantaj atunci când accesează piețele internaționale.

Model de politici și proceduri (instrumente practice)

Pentru a trece de la teorie la practică, organizațiile trebuie să transpună cerințele și bunele practici în documente operaționale interne – politici, proceduri, standarde, formulări. Aceste instrumente ghidează acțiunile concrete ale personalului și asigură repetabilitatea proceselor de securitate. În continuare, prezentăm **modele orientative** de politici și proceduri relevante pentru gestionarea riscurilor în lanțul de aprovizionare cu alimente. Aceste modele pot servi drept punct de plecare în dezvoltarea propriei documentații, care va fi apoi adaptată la specificul fiecărei organizații.

Politica de securitate cibernetică a lanțului de aprovizionare (exemplu de structură)

O astfel de politică definește angajamentele organizației față de securitatea relațiilor cu furnizorii și partenerii și stabilește cadrul pentru evaluarea și controlul riscurilor externe. Elementele cheie pot fi:

- **Scop și domeniu de aplicare:** De exemplu, *"Această politică stabilește cerințele de securitate cibernetică aplicabile lanțului de aprovizionare al companiei XYZ, inclusiv relațiile cu furnizorii, distribuitorii, furnizorii de servicii IT și alte terțe părți care gestionează date sau sisteme critice."*

- **Responsabilități:** Numirea unui *ofițer de securitate a lanțului de aprovizionare* (poate CISO sau un manager de risc) care supraveghează implementarea politicii. De asemenea, implicarea departamentelor de Achiziții (pentru includerea cerințelor de securitate în contracte), Legal (pentru clauze) și Operațiuni.

- **Cerințe de securitate pentru furnizori:** Lista principalelor așteptări din partea furnizorilor. Exemplu: *"Toți furnizorii critici trebuie să fie certificați ISO/IEC 27001 sau să demonstreze*

un nivel echivalent de controale de securitate. Furnizorii care accesează rețelele interne ale companiei trebuie să respecte politica noastră de parolă și MFA. Furnizorii de software vor furniza periodic atestări privind gestionarea vulnerabilităților (gestionarea patch-urilor) și ne vor anunța prompt despre orice încălcare a securității care ne poate afecta.".

- **Procesul de evaluare a riscurilor furnizorilor:** Angajamentul de a efectua evaluări periodice (de exemplu, anuale) de securitate pentru furnizorii din categorii critice și importante. Specificarea faptului că evaluările se bazează pe un *chestionar standard de securitate* (a se vedea lista de verificare a furnizorilor de mai jos) și, eventual, pe un audit independent pentru cele foarte critice.
- **Clasificarea furnizorilor în funcție de nivelurile de risc:** de exemplu: Nivelul 1 (critic) – servicii fără de care operațiunile se opresc, Nivelul 2 (semnificativ) – impact mediu, Nivelul 3 (non-critic). Politica poate spune că *"Pentru furnizorii de nivel 1, înregistrările de audit și planurile de continuitate sunt obligatorii, pentru nivelul 2, este necesar un răspuns la chestionarul de securitate, nivelul 3 – cerințe minime standard".*
- **Clauze contractuale de securitate: Ex:** *"Contractele cu furnizorii care prelucrează date sensibile sau au acces la sistemele noastre trebuie să includă un acord de confidențialitate, o clauză pentru notificarea incidentelor de securitate în termen de 24 de ore de la descoperire, dreptul nostru de a audita sau de a solicita teste de penetrare, obligația furnizorului de a implementa măsuri de securitate specificate (de exemplu: criptarea datelor în tranzit și stocare)."*
- **Gestionarea accesului terților:** Politica poate stabili că accesul de la distanță al furnizorilor (de exemplu, întreținerea echipamentelor) se face numai printr-un VPN securizat și cu aprobare prealabilă; conturile acordate terților sunt revizuite trimestrial; furnizorii nu primesc acces la date dincolo de minimul necesar (principiul privilegiului minim).
- **Monitorizare și revizuire:** angajamentul companiei de a monitoriza conformitatea furnizorilor (de exemplu, *"Vom revizui anual performanța de securitate a furnizorilor critici și vom discuta problemele de îmbunătățire în cadrul întâlnirilor periodice")* și de a revizui politica în sine la fiecare 2 ani sau la modificări legislative (de exemplu, apariția unui nou regulament).

Această politică ar urma să fie aprobată de conducere și comunicată atât intern (departamentelor implicate), cât și extern (furnizorilor, ca anexă la contracte, de exemplu, pentru a înțelege așteptările acestora).

Lista de verificare a evaluării securității furnizorilor (exemplu de listă de verificare)

O listă de verificare standardizată sau un chestionar folosit pentru a evalua furnizorii (mai ales înainte de contractare, dar și periodic):

- **Sistem de management al securității:** Furnizorul are politici de securitate documentate? Este certificat ISO 27001 sau alt standard recunoscut?
- **Guvernanță și resurse:** Există un ofițer de securitate clar la furnizor? Ce echipă/structură gestionează securitatea?
- **Controlul accesului:** Cum gestionează furnizorul accesul angajaților la sistemele și datele clienților? Folosește autentificarea cu doi factori? Are proceduri de revocare imediată a accesului atunci când angajații pleacă?

- **Protecția infrastructurii:** Furnizorul are măsuri de protecție perimetrală (firewall, IDS/IPS)? Criptează datele sensibile în tranzit și stocare? Folosește soluții antivirus/EDR pe stații de lucru și servere?
- **Managementul vulnerabilităților:** Ce proces are pentru aplicarea actualizărilor de securitate (gestionarea patch-urilor)? Cât durează aplicarea plasturilor critici după emitere? Își scanează periodic sistemele pentru vulnerabilități?
- **Backup și recuperare:** Are un plan de backup regulat pentru datele critice? Testează recuperarea datelor? În cazul unui atac, are capacitatea de a-și restabili operațiunile (există un plan de continuitate/DR)?
- **Răspuns la incidente:** Furnizorul are o echipă sau proceduri de răspuns la incidente? A avut incidente semnificative în trecut și cum le-a rezolvat? Este dispusă să notifice prompt beneficiarii afectați?
- **Protecția datelor și conformitatea legală:** Dacă furnizorul prelucrează date cu caracter personal sau confidențiale, respectă GDPR și alte reglementări? Au fost raportate încălcări de date autorităților?
- **Instruire și conștientizare:** Furnizorul își instruiește propriii angajați în securitate (de exemplu, phishing, igienă cibernetică)? Cât de des sunt cursurile de formare?
- **Localizarea datelor și accesul sub-furnizorilor:** Unde sunt stocate datele (centru de date local, cloud, UE/non-UE)? Folosește alți subcontractanți pentru serviciile oferite? Dacă da, există un flux de cerințe de securitate și pentru ei?
- **Audit și certificări suplimentare:** A fost supus recent unui audit de securitate terță parte? Are rapoarte SOC 2 (pentru servicii) sau certificări specifice industriei alimentare cu o componentă de siguranță (de exemplu, un sistem SCADA certificat pentru siguranță etc.)?

Această listă de verificare poate fi trimisă ca formular furnizorilor sau utilizată intern de către echipa de evaluare pentru a evalua furnizorul. Scopul este de a identifica lacunele: dacă, de exemplu, furnizorul nu are un plan de răspuns la incidente, acesta devine un subiect de discuție și o condiție pentru remediere. Nu toți furnizorii vor putea îndeplini 100% din cerințe, dar lista de verificare ajută *la calcularea unui scor de risc al furnizorului și la* luarea unei decizii în cunoștință de cauză (colaborăm sau nu, de ce compensații avem nevoie dacă colaborăm – de exemplu, încheiem o asigurare cibernetică suplimentară dacă furnizorul este slab într-un capitol).

Procedura de răspuns la incidente (model scurt)

Deși am detaliat procesul în capitolul anterior, aici vă prezentăm un format procedural clar, pas cu pas, care poate fi inclus în manualul intern:

1. **Detectarea incidentelor:** Orice angajat sau sistem automat care observă un eveniment suspect (alerte de securitate, comportament anormal al echipamentelor, mesaje de eroare neobișnuite etc.) trebuie să informeze imediat echipa IT/CSIRT (telefon intern de urgență, securitate e-mail... sau platforma de ticketing dedicată incidentelor). Timpul și natura observației vor fi notate.

2. **Evaluarea și clasificarea inițială:** CSIRT (sau IT on-call) evaluează rapid informațiile pentru a determina dacă este un **incident de securitate confirmat** și le asociază cu o severitate (critică, majoră, minoră) în funcție de impactul potențial. Dacă este vorba despre un *incident critic* (de exemplu, sistem de producție oprit de malware, acces neautorizat la datele rețetei,

atac în curs), managerul CSIRT și managementul relevant (management operațional) sunt alertați imediat.

3. **Izolare:** Echipa CSIRT execută acțiunile de izolare necesare în conformitate cu *Playbook-urile predefinite*. Ex: în caz de ransomware – deconectarea rețelei din fabrică de la VPN-ul central, oprirea anumitor switch-uri; în caz de exfiltrare detectată – blocarea conexiunilor de la IP-ul respectiv, suspendarea contului compromis etc. Se ia în considerare siguranța personalului și a echipamentelor (de exemplu, nu opriți brusc un sistem industrial dacă poate provoca daune fizice – comutați în modul manual controlat).

4. **Notificare internă și activare extinsă a echipei:** Un mesaj intern de incident (de exemplu, prin SMS sau telefon) este trimis membrilor echipei de răspuns (inclusiv reprezentant de producție, IT, management). În cazul în care incidentul întrerupe producția sau livrările, departamentul de logistică/vânzări este, de asemenea, notificat pentru a-și activa măsurile de continuitate (de exemplu, informarea clienților despre posibile întârzieri – sincronizare cu planul BCP).

5. **Investigare și eradicare:** Specialiștii tehnici analizează cauzele: colectează jurnale, mostre de malware, identifică vectorul de intruziune. În același timp, componentele rău intenționate sunt eliminate – ștergerea malware-ului, patch-urile vulnerabilităților, schimbarea parolei compromise. În cazul în care resursele interne sunt depășite, se contactează un partener extern de răspuns la incidente (dacă există un contract) sau se solicită ajutor din partea CERT național. Toate acțiunile și descoperirile sunt documentate.

6. **Recuperarea sistemului:** Odată ce amenințarea este considerată a fi eliminată, restaurează sistemele afectate din backup-uri curate (sau reconstruiește de la zero, după caz). Funcționalitatea și integritatea datelor sunt testate. Aceste sisteme sunt monitorizate intens după repunere în funcțiune pentru a detecta orice semne de persistență a atacatorului.

7. **Comunicare externă și notificări:** Dacă incidentul este semnificativ (criterii NIS2), în paralel cu pașii de mai sus, ofițerul NIS pregătește notificarea către autoritatea competentă (DNSC/CERT) conform formularului stabilit. Comunicările pot fi emise și către partenerii lanțului dacă aceștia sunt direct afectați (de exemplu, "furnizorul X – anunț: sistemele noastre sunt temporar indisponibile, nu ne puteți trimite comenzi electronic, utilizați telefonul"). Pentru mass-media/public, doar departamentul de comunicare emite declarații aprobate de conducere, dacă este cazul, menținând transparența și controlul informațiilor.

8. **Închiderea incidentului și raportul post-incident:** Liderul echipei CSIRT decide când incidentul poate fi declarat închis (criterii: sistemele sunt restaurate, nu mai există activități rău intenționate, operațiunile revin la normal sau se închid). Se convoacă o ședință de informare în care se analizează prețul acțiunilor. Raportul final al incidentului este completat, care include descrierea, impactul, cauzele principale, calendarul, măsurile luate, costurile și lecțiile învățate. Raportul este trimis conducerii superioare și, dacă legislația impune acest lucru (NIS2), autorităților. Orice recomandare (de exemplu, "este necesară actualizarea firewall-ului", "instruire personală suplimentară") este înregistrată și transformată în acțiuni concrete de îmbunătățire.

9. **Actualizarea și monitorizarea documentației:** Procedurile de securitate, planurile de răspuns sau de continuitate sunt actualizate în funcție de ceea ce s-a constatat (dacă a apărut o situație neprevăzută în planul actual, aceasta este acum adăugată). Echipa responsabilă

urmărește implementarea tuturor măsurilor corective (de exemplu, dacă s-a decis o segmentare suplimentară a rețelei, proiectul trebuie finalizat și verificat).

Această procedură se distribuie personalului relevant și se practică periodic (prin simulări de incidente). Fiecare membru al echipei știe astfel ce să facă atunci când are loc un incident real.

Plan de continuitate a activității (structură condensată)

Deși capitolul despre continuitate a detaliat pe larg conținutul unui BCP, iată o **structură tipică a scheletului** care poate fi folosită ca listă de verificare atunci când se întocmește planul:

- **Titlu și scop:** Planul de continuitate a afacerii pentru [organizație] – Asigurarea continuării operațiunilor critice (producția și distribuția de alimente) în cazul unui incident major.
- **Echipa de criză (BCM Team):** Nume, rol, contact (include Lider – Director de Operațiuni, Co-lider IT – CIO, Manager de Securitate, Manager de Producție, Manager de Logistică, Comunicare PR).
- **Analiza impactului – Procese critice:** (Tabel cu) procese esențiale, RTO, RPO, echipă responsabilă. Ex: Prelucrarea laptelui – RTO 4h, RPO 1h, Echipa de producție; Livrare cu amănuntul – RTO 8h, etc.
- **Măsuri de continuitate pe proces:**
  - *Producție:* generator electric de rezerva 250 kW per locație; stoc materie prima 2 zile; posibilitatea redistribuirii producției către fabrica din alt județ.
  - *IT (ERP, SCADA):* servere de replicare în timp real într-un centru secundar la 100 km; Plan de failover DNS; procedura manuală pentru emiterea comenzilor în cazul în care ERP nu este disponibil.
  - *Logistică:* contract cu transportatorul de rezervă dacă flota proprie nu este disponibilă; rute alternative în caz de infrastructură blocată.
  - *Aprovizionare:* listă de furnizori alternativi pentru ingredientele cheie (pudră de cacao, ambalaj), verificare și pre-aprobare; stoc minim de siguranță 7 zile pentru ambalare.
- **Proceduri imediate la debutul incidentului:** Lista de verificare a acțiunilor în primele 0-2 ore:
  1. Asigurarea siguranței fizice a personalului.
  2. Convocarea echipei de criză (telefon/WhatsApp).
  3. Evaluarea inițială a situației – ce proces este afectat, durata estimată.
  4. Decizia de a activa planuri alternative (de exemplu, mutarea producției).
  5. Notificări: personal intern (schimburi), parteneri critici, autorități (în caz de incident major).
- **Comunicare de criză:** Șabloane de mesaje:
  - Angajați interni: "Din cauza [incidentului], fabrica X funcționează la o capacitate redusă. Personalul din tura 2 este rugat să rămână acasă până la noi ordine. Vom reveni cu actualizări la ora 14:00."

- Clienților: "Întâmpinăm dificultăți operaționale temporare și livrările pot fi întârziate cu 1 zi. Vă asigurăm că echipa noastră lucrează continuu la remediere. Vă mulțumesc pentru înțelegere."
- Media (dacă este publică): Mesaj aprobat de PR și conducere, subliniind controlul situației și absența riscurilor pentru consumatori (dacă este cazul).

- **Resurse critice și contacte de urgență:** Lista furnizorului de generatoare, a tehnicienilor IT externi, a contactului pompierilor/poliției, a contactului DNSC (în cazul unui incident cibernetic major) etc.
- **Planuri detaliate pe scenarii majore:** (Anexe) Ex: Plan total de întrerupere IT, Plan de indisponibilitate a fabricii din cauze fizice, Plan de atac cibernetic, Plan de întrerupere a lanțului de aprovizionare. Fiecare cu pașii săi specifici.
- **Procedura de revenire la normal:** Cum să treceți de la modul de eroare la normal: reconectarea sistemelor la rețeaua principală, sincronizarea datelor din sistemele temporare, notificare "business as usual" pentru toată lumea, debriefing.
- **Revizuire și testare:** Când a fost ultimul test al planului, rezultate, când urmează următoarea actualizare.

Acest plan complet ar putea avea zeci de pagini cu anexe (inclusiv formulare standard, liste de inventar etc.), dar scheletul de mai sus ajută la structurare. **De asemenea, se recomandă un scurt plan de parcurs** – exemplu: un afiș A3 în camera de control din fabrică cu "În caz de incident major: 1) sunați managerul; 2) opriți sursa de alimentare după procedura X, dacă este necesar; 3) etc." – simplificat pentru reacție imediată, iar planul detaliat va fi consultat de echipa de criză pe parcurs.

Formular de notificare a incidentului (șablon)

După cum am exemplificat în capitolul anterior, un formular intern standardizat ajută la colectarea rapidă a informațiilor necesare raportării unui incident:

- Data, ora descoperirii:
- Cine a raportat inițial:
- Sistem/Departament afectat:
- Scurtă descriere a ceea ce se întâmplă (simptome):
- Acțiuni întreprinse până în prezent:
- Impactul curent (ce procese sunt oprite/încetinite, câte locații afectate, estimarea daunelor):
- Impact potențial dacă continuă (evaluarea riscurilor):
- Clasificarea severității interne: (Critic/Major/Minor, conform procedurii)
- Incident de securitate? (Da/Nu/Necesită investigație) – Dacă da, începe și procesul de notificare NIS.
- Manager de coordonare (numele managerului de incidente):
- Sunt necesare notificări externe? (Autoritatea NIS, poliția, clienții...):
- Aprobarea conducerii pentru notificarea externă: (nume, ora aprobării).

Formularul completat în primele ore devine baza pentru comunicările ulterioare. Poate fi o simplă pagină web internă sau un document standard pe care echipa de securitate îl completează și îl menține actualizat pe durata incidentului. Este important ca acest formular să fie accesibil și cunoscut de toți cei care pot observa incidente – de exemplu, un șef de tură de producție ar trebui să știe cum să completeze secțiunile de bază (ce vede, când, unde) și apoi personalul IT să adauge restul.

Modelele de mai sus nu sunt exhaustive, dar oferă un **punct de plecare pragmatic**. Fiecare organizație ar trebui să le detalieze și să le adapteze la propriul context. De exemplu, într-o companie mai mică, unele roluri se suprapun (aceeași persoană poate fi, de asemenea, responsabilă pentru continuitate și securitate), astfel încât politica și procedurile vor fi mai concise. Într-o corporație mare, pot fi elaborate documente separate pe sub-subiecte: Politica generală de securitate a informațiilor, plus Politica suplimentară pentru securitatea lanțului de aprovizionare; Planul de continuitate la nivel de companie plus planuri de continuitate IT și planuri de departament etc.

Important este ca aceste documente să nu rămână formale, ci să fie **implementate eficient**: personalul instruit în funcție de ele, procesele calibrate în funcție de ele, revizuite periodic. O politică frumos scrisă, dar neaplicată, are valoare zero în fața unui atac real. În schimb, un set de proceduri clare, practicate și înțelese de toți, poate reduce drastic confuzia și haosul în momentele critice, protejând astfel afacerea.

SECȚIUNEA 4. COOPERARE

Cooperarea cu partenerii și învățăminte de împărtășit

Un aspect special al răspunsului la incidente în lanțul de aprovizionare este **coordonarea cu partenerii din lanțul de aprovizionare**. Dacă incidentul dintr-o companie are repercusiuni directe asupra partenerilor (de exemplu, un furnizor nu poate livra sau un distribuitor nu primește date despre comandă), este esențial să-i informați rapid și să colaborați pentru a atenua efectele. Chiar și atunci când incidentul nu se propagă de la sine (nu malware-ul infectează alte companii), efectele de afaceri pot necesita o reacție sincronizată. Bunele practici recomandă includerea **protocoalelor de comunicare cu partenerii critici** în planurile de răspuns la incidente. De exemplu, un procesator are un acord cu principalii săi furnizori: "în cazul unui incident cibernetic care vă afectează capacitatea de a livra, vă rugăm să ne informați cât mai curând posibil prin canalul X, astfel încât să ne putem activa planurile de urgență". Și invers, compania de procesare se angajează să informeze furnizorii dacă suferă un atac care îi va afecta comenzile.

Un studiu ENISA a arătat că, într-un procent semnificativ de atacuri asupra lanțului de aprovizionare, clienții afectați știau mai multe despre modul în care a avut loc atacul decât furnizorii compromisi inițial (93% față de 38%), evidențiind un **deficit de maturitate în raportarea incidentelor la nivel de furnizor. Cu alte cuvinte, adesea furnizorii fie nu își dau seama cum au fost** piratați, fie nu comunică bine cu clienții despre asta, ceea ce agravează problemele. Ca atare, este nevoie de îmbunătățiri în acest domeniu: fluxul de informații despre incidente trebuie să curgă mai bine în ambele direcții de-a lungul lanțului.

La nivel european, există inițiative de creare **a unor comunități de partajare** a incidentelor și amenințărilor specifice sectorului alimentar. De exemplu, în alte sectoare există ISAC-uri (Information Sharing and Analysis Center) – centre prin care companiile dintr-un domeniu împărtășesc confidențial informații despre incidente și indicatori de compromis, pentru a se ajuta reciproc. Un Food-ISAC pan-european nu este încă bine definit, dar ENISA și autoritățile naționale încurajează mecanismele de cooperare informală. În România și Bulgaria, companiile alimentare esențiale pot participa la întâlnirile Grupului de Cooperare NIS sau la mese rotunde sectoriale organizate de autorități, unde schimbul de experiență legat de incidente este foarte valoros.

Formular de notificare a incidentelor (exemplu) – pentru a recapitula, mai jos este un scurt model care poate fi utilizat de entitățile alimentare:

- Data/ora constatării: 10.04.2025, 08:30.
- Entitate: Fabrica de procesare a produselor lactate XYZ (entitate importantă – sectorul alimentar).
- Contact raportor: Ioan Popescu – Manager Securitate IT, tel..., email...
- Descrierea incidentului: Ransomware detectat pe serverele de producție; Posturile operatorilor afișează un mesaj de răscumpărare.
- Impact: Producția în secțiunea de iaurt s-a oprit complet (linie blocată); Sistem ERP indisponibil; livrări estimate întârziate cu 1 zi.
- Acțiuni imediate: Linia de producție a fost oprită manual în siguranță; servere deconectate de la rețea; a notificat echipa internă de intervenție; Plan de continuitate activat (livrare din stoc).
- Cauza suspectată: E-mail de phishing primit cu o zi înainte, posibil deschis de un tehnician – investigație în curs.
- Impact transfrontalier: Posibil – livrările către 2 clienți BG vor fi întârziate (informații trimise acestora).

- Asistență necesară: Da – solicităm indicatori cunoscuți despre acest ransomware de la DNSC/CERT.
- Observații: Numele ransomware-ului afișat pare a fi "XYZLocker"; Nu există nicio indicație a datelor de exfiltrare până acum.

Acest tip de raport inițial ar fi prezentat prompt autorității. Ulterior, compania va urma proceduri interne și va informa autoritatea cu privire la evoluții (de exemplu: dacă descoperă că au fost furate date sau rețete de calitate, va actualiza notificarea, mai ales dacă este vorba despre date cu caracter personal – în cazul în care se încadrează în GDPR, necesitând notificarea separată către autoritatea de protecție a datelor).

În cele din urmă, un răspuns la incident bine gestionat face diferența între un eveniment neplăcut, dar depășit, și o criză devastatoare. Este esențial ca entitățile din lanțul alimentar să aibă planuri și echipe de răspuns pregătite, să nu ezite să coopereze cu autoritățile (acest lucru poate chiar reduce eventualele sancțiuni, dând dovadă de bună-credință) și să învețe din fiecare incident pentru a-și consolida apărarea. Răspunsul la incidente este, de asemenea, o oportunitate de a testa în practică robustețea planurilor de continuitate și de a consolida relațiile cu partenerii: trecând împreună printr-o criză, întregul lanț poate ieși mai puternic și mai rezistent.

Cooperarea transfrontalieră

Lanțurile de aprovizionare cu alimente funcționează adesea peste granițele naționale: produsele și materiile prime circulă între țări, iar companiile pot avea o prezență regională. Astfel, securitatea cibernetică a lanțului alimentar capătă o dimensiune transfrontalieră – incidentele și riscurile nu se opresc la frontieră, iar contracararea lor eficientă necesită cooperare internațională. Directiva NIS2 recunoaște această realitate, punând accentul pe **cooperarea și schimbul de informații** la nivelul UE între statele membre pentru a atinge un nivel comun ridicat de securitate cibernetică. În această secțiune, examinăm mecanismele de cooperare transfrontalieră relevante pentru România și Bulgaria în contextul lanțului de aprovizionare cu alimente și modul în care entitățile private pot beneficia de acestea.

Cadrul european de cooperare (Grupul de cooperare NIS, Rețeaua CSIRT, EU-CyCLONe)

La nivel strategic-politic, există **Grupul de cooperare NIS**, compus din reprezentanți ai statelor membre, ai Comisiei Europene și ai ENISA. Acest grup elaborează orientări, face schimb de informații politice, discută amenințările emergente și poate efectua **evaluări coordonate ale riscurilor pe lanțurile critice. De exemplu, în cazul în care există un val de atacuri asupra sectorului alimentar la nivel european, Grupul de cooperare ar putea iniția o analiză comună și ar putea formula recomandări sectoriale aplicabile în toate statele. Deși grupul operează la nivel guvernamental, rezultatele activității sale (rapoarte,** bune practici) ajung și la entități private sub formă de ghiduri și alerte.

La nivel operațional-tehnic funcționează **rețeaua CSIRT** , care reunește echipele naționale de răspuns la incidente (CERT). DNSC și CERT Bulgaria fac parte din această rețea, facilitând schimbul rapid de informații despre incidente, indicatori de compromis, tactici de atac etc. Pentru companii, acest mecanism se traduce prin faptul că, prin notificarea autorităților despre un incident grav, informațiile pot fi partajate (anonim, dacă sunt sensibile) către rețeaua CSIRT, alertând și alte țări. Într-o situație reală, dacă un atac vizează simultan mai multe companii alimentare din regiune (scenariu plauzibil cu ransomware sau atac țintit), rețeaua CSIRT permite coordonarea: de exemplu, DNSC poate notifica CERT Bulgaria și celelalte CERT-uri că amenințarea X a apărut, transmițând IoC (Indicatori de Compromitere). Astfel, companiile din aceste țări pot fi avertizate în avans. Acest schimb are loc aproape în timp real, în virtutea relațiilor de încredere construite în rețea.

O nouă componentă adusă de NIS2 este **EU-CyCLONe** (EU Cyber Crises Liaison Organization Network) – o structură concepută pentru a facilita gestionarea la nivel înalt a crizelor cibernetice

majore sau cu impact multiplu. EU-CyCLONe implică reprezentanți la nivelul autorităților naționale (factori de decizie, nu doar tehnicieni), care, în situații de criză gravă (de exemplu, un atac concertat asupra lanțurilor de aprovizionare cu alimente din mai multe țări, care duce la penurie), comunică și coordonează măsurile de răspuns. Acest lucru asigură că, dacă este necesar, există o viziune de ansamblu la nivelul UE, se alocă sprijin reciproc (poate chiar din punct de vedere logistic, nu doar informativ) și se trimit mesaje publice coerente pentru a evita panica. Desigur, EU-CyCLONe este rareori activat, doar la incidente de foarte mare amploare, dar existența sa evidențiază preocuparea de a trata securitatea cibernetică în sectorul alimentar ca pe o problemă de securitate a aprovizionării la nivel european.

Cooperare bilaterală și regională (cazul România-Bulgaria)

România și Bulgaria, în calitate de țări vecine și membre ale UE, au mai multe motive pentru a colabora îndeaproape în domeniul securității cibernetice, inclusiv pentru protecția lanțurilor alimentare regionale. Există câteva direcții concrete:

- **Schimb direct de informații CERT-to-CERT:** Indiferent de canalele oficiale ale UE, echipele naționale CERT au relații directe. De exemplu, dacă o companie din România raportează un atac care pare să provină din infrastructura din Bulgaria, DNSC poate contacta CERT Bulgaria pentru investigații suplimentare și invers. O astfel de cooperare are loc în mod obișnuit în cadrul rețelei balcanice de CERT.

- **Proiecte comune și schimb de bune practici:** România și Bulgaria pot colabora în proiecte europene (de exemplu, programe finanțate de Mecanismul pentru interconectarea Europei, Orizont Europa sau fonduri de cooperare transfrontalieră) axate pe creșterea securității cibernetice în sectorul alimentar. Există deja inițiative precum proiectul pilot derulat de DNSC în 2023-2024 privind implementarea Directivei NIS în sectorul producției și distribuției alimentare, la care au participat experți din ambele țări. Astfel de proiecte permit **evaluări comune ale riscurilor**, simulări ale incidentelor transfrontaliere și elaborarea de orientări sectoriale, beneficiind de expertiza combinată. Totodată, asigură crearea de contacte directe între companiile românești și bulgare din domeniu, facilitând schimbul de informații tehnice sau tactici defensive.

- **Exerciții regionale și cooperare militar-civilă:** În calitate de membre NATO, ambele țări participă la exerciții de simulare a atacurilor cibernetice (de exemplu, exercițiul anual al Coaliției Cibernetice) în care pot fi incluse și scenarii de infrastructură alimentară. În plus, există cooperare într-un format regional (Inițiativa celor Trei Mări, cooperarea SEE) care abordează și reziliența la nivel de infrastructură. Autoritățile de securitate cibernetică pot organiza *ateliere bilaterale* cu participarea sectorului privat, unde pot discuta lecțiile învățate din incidente și măsurile de prevenire. Un exemplu de bună practică ar fi un exercițiu comun simulat România-Bulgaria pe tema "Atac ransomware asupra unui producător transfrontalier de alimente", în care să se testeze procedurile de notificare reciprocă, împărțirea sarcinilor (cine informează clienții comuni, cum sunt asigurate livrările alternative) și coordonarea cu autoritățile ambelor state.

Beneficiile cooperării transfrontaliere sunt evidente: crește viteza de răspuns la amenințările regionale, evită duplicarea eforturilor (fiecare țară poate învăța din experiența celeilalte țări în loc să repete greșeli), iar lanțurile de aprovizionare – care funcționează adesea într-un mod integrat la nivel transfrontalier – beneficiază de un nivel coerent de protecție. Directiva NIS2 încurajează statele să își comunice reciproc **identificarea entităților esențiale/importante** atunci când acestea au operațiuni în mai multe țări, precum și să încheie acorduri de asistență reciprocă. România și Bulgaria, care au

un volum semnificativ de comerț agroalimentar bilateral, ar putea stabili un canal de consultare directă între DNSC și echivalentul bulgar pentru incidentele care afectează lanțurile alimentare. De exemplu, dacă un mare producător bulgar de carne, un furnizor important pentru piața românească, suferă un atac, autoritățile române ar putea oferi suport analitic sau resurse, știind că impactul se va resimți și pe plan intern.

În concluzie, **cooperarea transfrontalieră** acționează ca un multiplicator de forțe în gestionarea riscurilor cibernetice. Lanțul de aprovizionare cu alimente, ca infrastructură critică europeană, beneficiază de un front comun România-Bulgaria în fața amenințărilor. Fie că este vorba de politici armonizate, răspunsuri coordonate la incidente sau pur și simplu schimb de informații, acest efort comun consolidează securitatea ambelor țări și contribuie la obiectivul strategic al UE de a asigura o aprovizionare neîntreruptă și sigură cu alimente pentru toți cetățenii.

SECȚIUNEA 5. CONCLUZIILE

Lanțul de aprovizionare cu alimente se află astăzi la intersecția dintre infrastructurile critice tradiționale și noile provocări ale erei digitale. Pe de o parte, importanța sa pentru societate este incontestabilă – asigurarea alimentelor în mod constant și în siguranță este o condiție prealabilă fundamentală pentru stabilitate. Pe de altă parte, dependența tot mai mare de tehnologie și interconectarea extinsă fac ca acest sector să fie vulnerabil la amenințările cibernetice care, până de curând, nu se aflau pe lista riscurilor majore. Acest manual a evidențiat faptul că **securitatea cibernetică a lanțului alimentar nu mai poate fi tratată separat de managementul riscului operațional**, ci trebuie integrată organic, de la fermă și fabrică până la raftul magazinului.

Adoptarea **Directivei NIS2** și transpunerea acesteia în România (OUG 155/2024) și Bulgaria (legea în curs de actualizare) reprezintă un salt calitativ în abordarea acestor probleme. Pentru prima dată la nivel european, sectorul alimentar este recunoscut oficial ca parte a ecosistemului de securitate cibernetică, iar operatorii din domeniu – fie că sunt producători, procesatori sau distribuitori – sunt obligați să implementeze măsuri riguroase de securitate și să colaboreze cu autoritățile în caz de incidente. Acest cadru legal oferă un **impuls puternic**: dacă până acum unele companii ezitau să investească în securitate din motive de costuri, aceasta devine acum o cerință pentru conformitate și chiar supraviețuire pe piață (amenințarea cu amenzi substanțiale de până la 2% din cifra de afaceri nu poate fi ignorată).

Cu toate acestea, respectarea de dragul legii nu este suficientă. După cum am subliniat, **riscurile cibernetice evoluează constant**. Atacatorii își perfecționează tacticile, apar noi vulnerabilități, iar contextul geopolitic poate transforma infrastructura alimentară în ținte (gândiți-vă la atacurile orchestrate de state ostile menite să provoace penurie sau panică). Prin urmare, organizațiile trebuie să adopte o atitudine proactivă și anticipativă, depășind minimul impus de NIS2. Implementarea standardelor internaționale, parteneriatul strâns cu experții în securitate, testarea periodică a rezilienței (prin audituri, pentest, exerciții de echipă roșie) și îmbunătățirea continuă sunt elementele unui **cerc virtuos** de maturitate în securitate.

Acest manual a oferit atât o perspectivă teoretică, cât și practică asupra elementelor esențiale: de la **cadrul legal** (ce ne obligă să acționăm), la **managementul riscurilor** (cum identificăm și prioritizăm pericolele), la **securitatea cibernetică specifică lanțului alimentar** (care sunt vulnerabilitățile concrete și cum le abordăm), la **continuitatea operațională** (cum să ne pregătim pentru incidentul inevitabil) și **răspunsul** la incidente (ce facem când se întâmplă), la **cooperarea internațională** (pentru că nu suntem singuri în această luptă) și **la bune practici** (instrumentele pe care le avem la dispoziție, deja testate de alții). Am integrat exemple reale – din fericire, nu foarte numeroase până acum în industria alimentară – care, totuși, servesc drept avertismente timpurii. Atacurile asupra distribuitorilor de alimente și a producătorilor de băuturi din ultimii ani ne arată că **amenințarea este prezentă și actuală**.

România și Bulgaria, prin particularitățile lor, împărtășesc atât provocări, cât și oportunități. Ambele au trecut printr-o digitalizare accelerată, dar se confruntă și cu infrastructuri IT moștenite și uneori cu resurse limitate în companii, în special în zona IMM-urilor. Transpunerea NIS2 vine pentru a egaliza condițiile de concurență – toți actorii importanți trebuie să atingă un anumit nivel de securitate. Colaborarea dintre companii, sectoare și autorități va fi esențială pentru ridicarea întregului ecosistem la nivelul necesar. DNSC din România și viitoarea autoritate NIS2 din Bulgaria trebuie să continue să ofere îndrumări (ghiduri sectoriale, instruiri, exerciții) și să acționeze ca parteneri de încredere ai industriei, nu doar ca organisme de control.

La nivel macro, putem spune că **securitatea lanțului de aprovizionare cu alimente este o problemă europeană comună**, iar soluțiile se construiesc prin efort colectiv. Standardizarea celor mai bune practici, schimbul rapid de informații despre amenințări (printr-o rețea paneuropeană robustă) și crearea unei culturi a rezilienței vor face diferența în fața atacurilor de mâine. Nu trebuie să așteptăm

un incident catastrofal pentru a acționa; Dimpotrivă, scopul nostru este să o prevenim sau, dacă nu poate fi prevenită, **să-i limităm drastic impactul**.

În cele din urmă, ne amintim câteva **mesaje cheie**:

- *Conștientizare:* Lanțul de aprovizionare cu alimente este expus unor riscuri cibernetice semnificative. Managementul organizațiilor din domeniu trebuie să recunoască acest fapt și să-l trateze ca pe un risc major de afaceri, nu ca pe o chestiune strict tehnică.
- *Pregătire:* Implementarea structurilor de management al riscurilor și securității (politici, echipe, procese) este esențială. Nu putem improviza în mijlocul unei crize; Planurile bine puse în aplicare economisesc timp și resurse și protejează reputația.
- *Prevenirea prin colaborare:* Nicio entitate nu poate obține singură securitate absolută. Parteneriate cu furnizorii pentru a-și îmbunătăți securitatea, participarea la comunitățile de schimb de informații, alinierea la standarde comune – toate acestea ridică nivelul de securitate pentru întregul lanț.
- *Răspuns eficient:* Când apar incidente, modul în care reacționăm face diferența. Comunicarea transparentă, intervenția rapidă și raportarea corectă către autorități reduc daunele și accelerează revenirea la normal.
- *Învățare continuă:* Securitatea cibernetică este un proces continuu. După fiecare exercițiu sau incident, tragem concluzii și ne îmbunătățim. Tehnologia evoluează, amenințările evoluează – și noi trebuie să evoluăm.

Prin aplicarea cunoștințelor și instrumentelor prezentate în acest manual, managerii IT, ofițerii de securitate și toți profesioniștii implicați în lanțul de aprovizionare cu alimente pot dezvolta un **sistem robust de management al riscurilor cibernetice**. Acesta va proteja nu numai interesele economice ale companiilor, ci și bunăstarea cetățenilor care depind de serviciile lor. Miza este încrederea publicului că, indiferent de provocări – fie că este vorba de pandemii sau atacuri cibernetice – **alimentele vor continua să ajungă la masa tuturor** în siguranță.

În concluzie, securitatea cibernetică a lanțului de aprovizionare cu alimente nu este doar o cerință de conformitate legală, ci o responsabilitate față de societate. România și Bulgaria, împreună cu partenerii lor europeni, fac pași importanți în această direcție, iar succesul va depinde de angajamentul comun al autorităților, al sectorului privat și al mediului academic. Acest manual speră să fi contribuit la consolidarea cunoștințelor și să ofere un ghid util pentru toți cei implicați în protejarea unui sector atât de vital. Haideți să abordăm aceste provocări cu seriozitate, cooperare și perseverență, pentru un viitor în care reziliența cibernetică devine o a doua natură a lanțului de aprovizionare cu alimente.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

Bibliografie

- Directiva (UE) 2022/2555 (NIS2) (https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=ro).
- OUG 155/2024 (România) – Ordonanță de urgență pentru securitate cibernetică (https://legislatie.just.ro/Public/DetaliiDocumentAfis/293121).
- ENISA – *Bune practici pentru securitatea cibernetică a lanțului de aprovizionare*, 2023 (https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity)
- Burcu Yasar – *Securizarea spațiului cibernetic european: este sectorul alimentar și agricol critic?* CiTiP Blog KU Leuven (https://www.law.kuleuven.be/citip/blog/securing-european-cyberspace-is-the-food-and-agriculture-sector-critical/)
- Roaliment.ro – *Industria alimentară, în vizorul hackerilor: o urgență ignorată*, (https://www.roaliment.ro/procesare/industria-alimentara-in-vizorul-hackerilor-securitatea-cibernetica-devine-o-urgenta-ignorata/).
- Digital Watch – *Legea bulgară privind securitatea cibernetică – actualizări și transpunerea NIS2*, (https://cyberupgrade.net/blog/compliance-regulations/nis2-directive-regulations-and-implementation-in-bulgaria/)
- Ogletree Deakins – *Directiva NIS2 a UE: ... Managementul riscurilor, raportarea incidentelor și sancțiunile* (https://ogletree.com/insights-resources/blog-posts/the-eus-nis2-directive-covered-entities-compliance-monitoring-risk-management-incident-reporting-and-penalties/).
- ENISA – *Peisajul amenințărilor 2022* (https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022).
- Grupul de cooperare NIS – *Cipru: Bune practici în securitatea lanțului de aprovizionare*, Bowcut, S. *"Protejarea aprovizionării: securitatea cibernetică în alimentație și agricultură"*, Food and Ag-ISAC, *"Food and Agriculture Sector 2024 Cyber Threat Trends"*, rezumat al raportului. (CybersecurityGuide.org)
- TXOne Networks, *"Securitatea cibernetică în sectorul alimentar: cum atacurile cibernetice pot perturba lanțul de aprovizionare"* (https://www.txone.com/blog/how-cyberattacks-disrupt-food-supply-chain)
- ISA Global Cybersecurity Alliance (ISAGCA), *"Securitatea și segmentarea sistemului de control industrial (ICS)"*, (https://gca.isa.org/blog/industrial-control-system-ics-security-and-segmentation)
- MEGA International, *"Pașii procesului de management al riscului (ISO 31000)"*, (https://www.mega.com/blog/what-is-risk-management-process)
- C-Risk, *"ISO 27005 – Managementul riscurilor de securitate a informațiilor (prezentare generală a pașilor)"*, (https://www.c-risk.com/blog/iso-27005)
- CISA, *"Exercițiul Cyber Storm VIII (sectorul alimentar și agricol)"*, (https://www.cisa.gov/resources-tools/programs/cyber-storm).

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.