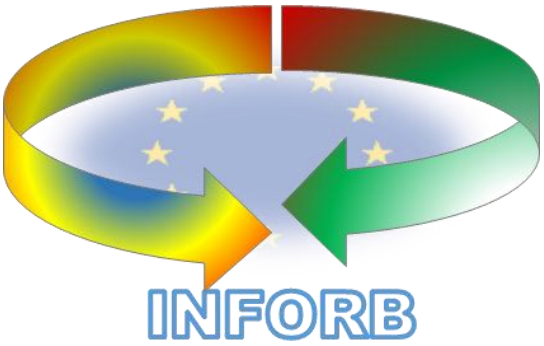

GHID PRACTIC PENTRU CREȘTEREA SECURITĂȚII CIBERNETICE ÎN ORGANIZAȚIILE ȘI ENTITĂȚILE DIN SECTORUL ALIMENTAR

LIVRABIL D2.3

Versiunea 1.0

REZUMAT

Acest ”Ghid practic pentru creșterea securității cibernetice în organizațiile și entitățile din sectorul alimentar” oferă un cadru practic și structurat pentru organizațiile din sectorul alimentar care doresc să-și îmbunătățească securitatea cibernetică în conformitate cu cerințele Directivei NIS 2 și cu nevoile specifice ale industriei. Scopul principal este de a crește securitatea cibernetică, de a proteja sistemele, rețelele și datele organizațiilor din sectorul alimentar, de a asigura conformitatea, de a alinia practicile de securitate la cerințele NIS2, GDPR și alte reglementări relevante, de a sprijini reziliența operațională, de a dezvolta capacitatea organizațiilor de a preveni, detecta și răspunde la incidentele cibernetice, de a proteja reputația și încrederea clienților și de a evita breșele de securitate care ar putea afecta încrederea clienților și partenerilor. Acest ghid este un instrument esențial pentru organizațiile din sectorul alimentar care doresc să-și îmbunătățească securitatea cibernetică și să respecte reglementările europene. Prin abordarea riscurilor cibernetice într-o manieră proactivă și structurată, organizațiile pot proteja activele critice, pot asigura siguranța alimentară și pot menține încrederea clienților și a partenerilor de afaceri.

PROJECT:
101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Informații privind controlul documentelor

Setări	Valoare
Titlul documentului:	Ghid practic pentru creșterea securității cibernetice în organizațiile și entitățile din sectorul alimentar
Numărul proiectului:	101128047
Numele proiectului:	Implementarea Directivei NIS în sectorul producției, procesării și distribuției alimentelor din România și Bulgaria.
Acronimul proiectului:	INFORB
Documentul autorului/autorilor:	Gabriel Hîmpă, Silviu-Nicolae Dorobanțu, Gergana Rakova, Eli Kuyamova, Panayotka Panayotova
Identificator livrabil:	D2.3
Data limită de livrare:	30.06.2025
Data livrării:	24.06.2025
Manager de proiect:	Constantin CĂLIN
Versiunea documentului:	V1.0
Sensibilitate:	PU-Public
Dată:	23.06.2025

Evaluatori de documente și evaluatori

Nume	Rol	Acțiune	Dată
Gabriel Hîmpă	Liderul WP 2	Proiect de document creat	11.12.2024
Gabriel Hîmpă	Liderul WP 2	Versiunea originală (DNSC)	10.04.2025
Gergana Rakova	Proiect	Versiune de actualizare (BGMEG)	17.06.2025
Eli Kuyamova	Expert în proiecte și securitate cibernetică		
Panayotka Panayotova	Lider de proiect BG	Contribuția BG agreată	18.06.2025
Consiliul consultativ de experți	Evaluare	Versiunea convenită	20.06.2025
Constantin Călin	Manager de proiect	Documentul final convenit și livrat	24.06.2025

Istoricul documentelor

Revizie	Dată	Creat de	Scurtă descriere a modificărilor
V0	10.04.2025	Liderul WP 2	Document creat
V0.1	10.05.2025	Liderul WP 2	Rectificarea documentului actualizat cu informații
V0.1.1	15.05.2025	Lider al WP 2 și expert în securitate cibernetică	Actualizați documentul
V0.1.2	15.05.2025	Expert în securitate cibernetică	Limba engleză actualizată
V0.1.3	18.06.2025	Coordonator/Lider de proiect	Limba engleză actualizată de experți bulgari
V1.0	23.06.2025	Liderul WP 2	Documentul final versiunea 1

Cuprins

INTRODUCERE

Acest "Ghid practic pentru îmbunătățirea securității cibernetice în organizațiile din sectorul alimentar" (denumit în continuare "Ghidul") a fost elaborat în cadrul proiectului INFORB – "Implementarea Directivei NIS în sectorul producției, procesării și distribuției alimentelor din România și Bulgaria" – cofinanțat de Comisia Europeană. Ghidul își propune să sprijine entitățile în abordarea riscurilor de securitate cibernetică relevante pentru sectorul alimentar prin alinierea practicilor lor la Directiva (UE) 2022/2555 (NIS2), GDPR și la standardele relevante (ISO/IEC 27001, HACCP, ISO 22000, IEC 62443). Acesta promovează identificarea entităților critice și a infrastructurilor digitale, în special în lumina amenințărilor tot mai mari la adresa sistemelor de control industrial (ICS/SCADA), a tehnologiei operaționale (OT) și a lanțurilor de aprovizionare digitale.

Aceasta este prima resursă structurată, axată pe sectorul alimentar ca domeniu critic nou recunoscut în cadrul NIS2. Ghidul pune accentul pe securitatea bazată pe riscuri, conformitatea cu reglementările, continuitatea afacerii și siguranța alimentară ca piloni interconectați ai rezilienței cibernetice.

Obiectivul principal al proiectului este de a identifica entitățile economice și de a le clasifica ca entități esențiale și importante într-un sector de importanță critică, de a evalua și asigura securitatea cibernetică, inclusiv lanțul de aprovizionare, în special pentru sectorul "Producție, procesare și distribuție a alimentelor" (denumit în continuare sectorul "alimente").

Ghidul este un instrument important pentru întreprinderile economice din sectorul alimentar, ajutându-le să își identifice în timp util vulnerabilitățile specifice în lumina amenințărilor din mediul digital în care operează, să își îmbunătățească și să-și consolideze continuu capacitățile de securitate cibernetică, astfel încât să poată gestiona eficient riscurile de securitate cibernetică.

Scop

Scopul principal al acestui ghid este de a sprijini organizațiile din sectorul alimentar în îmbunătățirea posturii lor de securitate cibernetică prin:

- Protejarea activelor digitale și fizice legate de producția, procesarea și distribuția alimentelor;
- Asigurarea confidențialității, integrității și disponibilității (CIA) a datelor sensibile și a sistemelor operaționale;
- Prevenirea, detectarea și răspunsul la amenințările cibernetice care pot compromite siguranța alimentară, continuitatea operațională sau încrederea consumatorilor;
- Promovarea integrării securității cibernetice în cadrele existente de siguranță alimentară, cum ar fi HACCP și ISO 22000;
- Sprijinirea conformității cu NIS2, GDPR și legislația națională privind securitatea cibernetică (de exemplu, OUG 155/2024).

Ghidul își propune, de asemenea, să crească gradul de conștientizare, să construiască reziliența organizațională și să promoveze o cultură proactivă a securității cibernetice în rândul personalului tehnic și non-tehnic.

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.

Obiective

Creșterea gradului de conștientizare cu privire la riscurile cibernetice

Acest obiectiv își propune să sensibilizeze organizațiile economice din sectorul alimentar cu privire la riscurile cibernetice specifice acestui domeniu prin evidențierea amenințărilor cibernetice (de exemplu, atacuri ransomware, breșe de date sau compromiterea sistemelor de control industrial) și impactul acestora asupra siguranței alimentare, sănătății populației, operațiunilor, precum și reputației entității economice.

Protecția infrastructurii critice

Un al doilea obiectiv important este **identificarea și protejarea infrastructurilor critice** care au un impact semnificativ asupra securității cibernetice și a bunei funcționări a serviciilor esențiale. Acestea pot include sisteme de prelucrare a datelor, rețele de distribuție, sisteme de management al producției etc.

Furnizarea unui cadru practic de acțiune

În acest context, să furnizeze măsuri clare și executorii pentru evaluarea vulnerabilităților, estimarea amenințărilor, identificarea riscurilor probabile și punerea în aplicare a măsurilor de evaluare și gestionare a riscurilor de securitate cibernetică prin recomandări pentru protecția sistemelor informatice, a rețelelor și a datelor, inclusiv utilizarea firewall-urilor, criptarea comunicațiilor, gestionarea accesului și actualizările periodice.

Asigurarea conformității cu reglementările specifice industriei

Facilitarea alinierii la cerințele de reglementare precum NIS2, GDPR și legislația națională (OUG 155/2024, Legea 58/2023). Ghidul sprijină înțelegerea obligațiilor de conformitate, implementarea controalelor adecvate și utilizarea instrumentelor pentru notificare, documentare și pregătire pentru audit.

Protejarea lanțului de aprovizionare digital

Scopul este de a sprijini organizațiile în securizarea lanțului de aprovizionare digital și a relațiilor cu partenerii. Acest lucru poate fi realizat cu ajutorul recomandărilor pentru evaluarea securității cibernetice a furnizorilor și a colaborării eficiente pentru a minimiza riscurile.

Creșterea rezilienței operaționale

Obiectiv: Îmbunătățirea capacității organizațiilor de a preveni, detecta și răspunde la incidentele cibernetice.

Detalii: Dezvoltarea planurilor de răspuns la incidente și de continuitate a afacerii, precum și implementarea practicilor de monitorizare continuă.

Promovarea educației și formării

Obiectiv: Îmbunătățirea gradului de conștientizare și competențele de securitate cibernetică ale angajaților prin instruire continuă, simulări de phishing și educație specifică rolului. Asigurarea incluziunii atât a personalului IT, cât și a celor non-IT, în special a celor care lucrează cu medii OT/ICS. Promovarea unei culturi a securității prin comportament.

Detalii: Furnizarea de resurse și recomandări pentru programele de formare și conștientizare a angajaților.

Protejarea datelor sensibile și a confidențialității

- **Obiectiv**: Asigurarea confidențialității, integrității și disponibilității datelor sensibile.

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.

- **Detalii**: Implementarea măsurilor de protecție a datelor, cum ar fi criptarea, backup-urile regulate și gestionarea accesului.

Prevenirea atacurilor cibernetice și minimizarea impactului

- **Obiectiv**: Reducerea riscului de atacuri cibernetice și limitarea impactului acestora asupra operațiunilor.
- **Detalii**: Recomandări pentru prevenirea atacurilor (de exemplu, utilizarea soluțiilor antivirus, detectarea intruziunilor) și planificarea răspunsurilor rapide.

Sprijinirea inovării și a adaptabilității

- **Obiectiv**: Încurajarea organizațiilor să adopte tehnologii și practici inovatoare de securitate cibernetică.
- **Detalii**: Promovarea utilizării soluțiilor avansate, cum ar fi inteligența artificială pentru detectarea timpurie a amenințărilor și adaptarea la noile riscuri cibernetice.

Protejarea reputației și încrederii clienților

- **Obiectiv**: Menținerea și consolidarea încrederii clienților și partenerilor de afaceri prin asigurarea unui mediu digital sigur.
- **Detalii**: Evitarea breșelor de securitate care ar putea afecta reputația și transparența în gestionarea incidentelor.

Facilitarea colaborării și a schimbului de informații

- **Obiectiv**: Încurajarea colaborării la nivel sectorial prin platforme de partajare a informațiilor despre amenințări, participarea la ISAC (Centre de Partajare și Analiză a Informațiilor) și coordonarea DNSC. Promovarea canalelor de încredere pentru raportare și sprijin reciproc.
- **Detalii**: Promovarea schimbului de informații despre amenințări și vulnerabilități între entități.

Furnizarea de instrumente și resurse practice

- **Obiectiv**: Furnizarea de instrumente, liste de verificare și exemple de bune practici pentru a facilita punerea în aplicare a măsurilor de securitate.
- **Detalii**: Ghidul include resurse care pot fi aplicate imediat în organizații, cum ar fi șabloane de politici de securitate sau planuri de răspuns la incidente.

Adaptarea la noile tendințe și amenințări

- **Obiectiv**: Să ajute organizațiile să rămână la curent cu amenințările cibernetice în evoluție și să-și adapteze strategiile de securitate.
- **Detalii**: Furnizarea de îndrumări pentru monitorizarea tendințelor și inovațiilor în materie de securitate cibernetică.

Obiectivele acestui ghid sunt **practice, relevante și adaptate nevoilor sectorului alimentar**. Scopul lor este de a oferi organizațiilor un cadru clar și aplicabil pentru îmbunătățirea securității cibernetice, asigurând în același timp conformitatea cu reglementările și protejând activele critice. Prin urmare, acest ghid este un instrument esențial pentru construirea unei culturi de securitate cibernetică și asigurarea rezilienței organizațiilor într-un mediu digital din ce în ce mai complex.

Cadrul legislativ și de reglementare

- **OUG nr. 155/2024** în România – stabilește obligațiile legale pentru entitățile din sectoarele critice, printre care:

- articolele 5-8: definițiile entităților în cauză;
- articolele 14-15: cerințe de securitate cibernetică;
- Articolele 16-18: notificarea incidentelor către DNSC.

- **Legea nr. 58/2023** în România – consolidează structura instituțională națională pentru apărarea cibernetică și introduce obligații de audit și partajare a riscurilor.
- **Legea privind securitatea cibernetică din Bulgaria** care a transpus directiva NIS1 inițială, stabilind un cadru pentru identificarea operatorilor de servicii esențiale și reglementarea măsurilor de securitate.
- **Ordonanța Bulgariei privind cerințele minime pentru securitatea rețelelor și a informațiilor stabilită prin Legea privind securitatea cibernetică**. Ca document legal, acesta prevede în mod specific diferitele domenii ale securității rețelelor și a informațiilor (securitatea cibernetică) pe care trebuie să le respecte fiecare subiect care intră sub jurisdicția sa, inclusiv administrația publică (cu excepția celor enumerate la articolul 5). Toate entitățile care intră sub jurisdicția sa sunt obligate să implementeze și să respecte principiile și cerințele tehnice stabilite în Ordonanță, inclusiv, dar fără a se limita la: managementul securității rețelelor și a informațiilor; documentație informativă; clasificarea informațiilor; managementul lanțului de aprovizionare; managementul riscului; gestionarea activelor informaționale; securitatea resurselor umane; managementul schimbării; relațiile cu terții; filtrarea traficului; criptografie; administrație; controlul accesului; acces de la distanță; protecția software-ului și hardware-ului; protecție împotriva software-ului rău intenționat; protecția aplicațiilor web și a serverelor; Protecție DNS; protecție fizică; și altele. Documentul obligă subiecții care intră sub jurisdicția sa să ia măsuri specifice pentru gestionarea riscurilor de securitate a rețelelor și a informațiilor, care includ adoptarea unui proces documentat de evaluări periodice ale riscurilor pe baza unei metodologii de evaluare a riscurilor, aprobată de subiect.
- **Regulamentul (UE) 2022/2554 (DORA)** – aplicabil entităților financiare și TIC colaboratoare relevante.
- **Ordine DNSC emise în 2024**:
  - Ordin privind **criteriile și pragurile de perturbare**;
  - Comanda pe **procesul de notificare și PlatformaNIS2@RO (denumită NIS2@RO)**;
  - Ordinul privind **evaluarea scorului de risc și a nivelului CyFUN aplicabil**.

Instrumente oficiale:

- **NIS2@RO** – înscriere, informare și notificare DNSC;
- **Formulare standard de autoevaluare** – publicate de DNSC.
- **Formulare standard pentru autoevaluare** în Bulgaria în conformitate cu Ordonanța bulgară privind cerințele minime pentru securitatea rețelelor și a informațiilor.

Transpunerea în România și Bulgaria

- **Transpunerea în România**
  - Odată cu publicarea **Ordonanței de urgență nr. 155/2024**, România a transpus **Directiva (UE) 2022/2555 (NIS2),** stabilind cerințe clare pentru protecția rețelelor și sistemelor informatice în spațiul cibernetic civil național. Legea **nr. 58/2023** consolidează componenta de apărare și coordonare cibernetică.
- **Transpunerea în Bulgaria**

- Ministerul bulgar al guvernării electronice a pregătit un proiect de modificare a Legii privind securitatea cibernetică. Acest document a fost prezentat Parlamentului în iulie 2024 spre adoptare, cu scopul de a transpune noile cerințe NIS2 în legislația națională.
- Până la termenul european (17 octombrie 2024), Bulgaria nu finalizase adoptarea amendamentelor, astfel încât la acea dată transpunerea era încă nefinalizată, iar proiectul era în dezbatere parlamentară. Procesul legislativ continuă spre sfârșitul anului 2024 și se află în etapa finală a acestei adoptări.
- Până la intrarea în vigoare a modificărilor NIS2, Bulgaria continuă să aplice prevederile legislației existente (NIS1).

Aspecte generale despre ghid

Acest ghid este elaborat pentru a sprijini entitățile economice din sectorul alimentar în:

- înțelegerea statutului juridic (entitate esențială/importantă);
- evaluarea riscurilor cibernetice și aplicarea unor niveluri proporționale de măsuri pentru a le reduce la minimum;
- alinierea la cele mai bune practici internaționale (Cyber Fundamentals, ISO/IEC 27001, NIST CSF);
- îndeplinirea obligațiilor de notificare, audit și reziliență operațională.

Se adaugă, de asemenea, următorul text:

- Context geopolitic și economic care crește riscul de atacuri asupra infrastructurii alimentare;
- Necesitatea interoperabilității între sistemele IT și OT;
- Nevoia urgentă de a forma o cultură organizațională a securității în rândul lucrătorilor non-IT.

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.

SECȚIUNEA 1. BAZELE SECURITĂȚII CIBERNETICE ÎN SECTORUL ALIMENTAR

Securitatea cibernetică în sectorul alimentar se referă la protecția sistemelor informatice, a rețelelor, a datelor și a infrastructurilor digitale utilizate în producția, prelucrarea, distribuția și comercializarea produselor alimentare. Aceasta implică implementarea unor măsuri și practici care previn, detectează și răspund la amenințările cibernetice care ar putea afecta operațiunile organizației, siguranța alimentară, confidențialitatea datelor și reputația.

1.1. Ce este securitatea cibernetică?

1.1.1. Definiție:

- Securitatea cibernetică, denumită și securitate digitală sau IT, cuprinde politici, procese, tehnologii și factori umani care vizează protejarea sistemelor informatice, a rețelelor, a dispozitivelor și a datelor împotriva amenințărilor cibernetice, cum ar fi accesul neautorizat, încălcarea datelor, malware-ul sau întreruperea serviciului. Asigură confidențialitatea, integritatea și disponibilitatea (CIA) a activelor digitale și susține continuitatea afacerii. Securitatea cibernetică este practica de protejare a sistemelor informatice, a rețelelor, a dispozitivelor și a datelor împotriva atacurilor cibernetice, a accesului neautorizat și a altor amenințări.

1.1.2. Scop

- Pentru a păstra confidențialitatea, integritatea și disponibilitatea (CIA) a informațiilor și sistemelor, asigurând operațiuni neîntrerupte, protecția datelor și reziliența împotriva amenințărilor cibernetice care ar putea compromite siguranța alimentară, lanțurile de aprovizionare sau respectarea obligațiilor legale.
- **Documente oficiale:** Verificarea înregistrărilor oficiale ale entității în registrul comerțului și în alte baze de date guvernamentale pentru a confirma codurile NACE sub care este înregistrată entitatea.

1.2. Specificul sectorului alimentar

1.2.1 Activele critice din sectorul alimentar includ:

- **Activele critice din sectorul alimentar includ:**
- **Sisteme de control industrial (ICS)/SCADA:** Gestionați liniile de producție automatizate și controlul temperaturii în procesarea alimentelor;
- **Tehnologie operațională (OT):** mașini și senzori utilizați în sortarea, ambalarea sau depozitarea alimentelor;
- **Date sensibile:** informații despre clienți, rețete proprietare, contracte cu furnizorii și documentație de control al calității ;
- **Dispozitive IoT:** termometre inteligente, debitmetre și senzori de umiditate conectați la servicii cloud ;
- **Platforme de management al lanțului de aprovizionare:** Sisteme digitale care coordonează achizițiile, logistica și livrarea.

1.2.2 Principalele amenințări cibernetice din sectorul alimentar includ:

- **Atacuri ransomware** care opresc operațiunile și criptează datele critice;
- **Atacuri asupra lanțului de aprovizionare,** în care software-ul sau hardware-ul terț introduce vulnerabilități;
- **Manipularea sistemelor ICS/OT,** care pot modifica temperatura, igiena sau nivelurile de ingrediente, punând în pericol siguranța alimentară;

- **Încălcări ale datelor** care expun datele clienților, proprietatea intelectuală sau informațiile de trasabilitate;
- **Comenzi false și fraudă cu facturi** care vizează sistemele de achiziții;
- **Atacuri Denial-of-Service (DoS/DDoS)** care afectează platformele logistice sau controlul stocurilor.

1.3. Principii de securitate cibernetică (componente-cheie)

- **Confidențialitate**: Prevenirea accesului neautorizat la date sensibile, cum ar fi rețete, contracte și înregistrări medicale.
- **Integritate:** Garantarea faptului că parametrii de producție, jurnalele de temperatură și datele lotului sunt exacte și nemodificate.
- **Disponibilitate:** Asigurarea faptului că serviciile digitale (de exemplu, interfețe ICS, sisteme ERP, portaluri pentru clienți) sunt accesibile atunci când este necesar pentru continuitatea operațională.

1.4. Riscuri cibernetice în sectorul alimentar

- **Ransomware:** Poate întrerupe producția, depozitarea sau livrarea.
- **Phishing și inginerie socială:** poate duce la acces neautorizat sau fraudă la facturi.
- **Atacuri ICS/SCADA:** Pot compromite calitatea producției, trasabilitatea alimentelor sau controalele de igienă.
- **Amenințări din interior:** scurgeri de date intenționate sau accidentale de către angajați.
- **Vulnerabilități terțe:** exploit-uri introduse prin parteneri sau furnizori.
- **Sisteme moștenite fără patch-uri:** Comune în fabricile de alimente de lungă durată.

1.5. Măsuri de securitate cibernetică

- **Firewall-uri și IDS/IPS:** Filtrați traficul rău intenționat și detectați încercările de intruziune.
- **Criptare:** Se aplică datelor sensibile, atât în stocare, cât și în timpul transmiterii.
- **Controlul accesului:** Implementați controlul accesului bazat pe roluri (RBAC) și autentificarea cu mai mulți factori (MFA).
- **Gestionarea corecțiilor:** Aplicați actualizările de securitate cu promptitudine, în special pentru componentele ICS și OT.
- **Securitate fizică:** Protejați dispozitivele ICS împotriva accesului fizic neautorizat.
- **Segmentarea rețelei:** Izolați rețelele de producție de rețelele de afaceri sau externe.

1.6. Conformitate cu reglementările

- **ORDONANȚA DE URGENȚĂ nr. 155 din 30 decembrie 2024** (România) privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice în spațiul cibernetic civil național, definește obligațiile legale, pragurile de incidente, utilizarea platformei DNSC.;
- **Modificarea Legii privind securitatea cibernetică (Bulgaria), nr. 51-402-01-17**, prezentată de Consiliul de Miniștri Adunării Naționale la 12 decembrie 2024, adoptată la primul vot la 20 februarie 2025.
- **NIS 2**: Directiva UE privind securitatea rețelelor și a sistemelor informatice, care impune cerințe stricte pentru securitatea Cibernetică, aplică managementul riscurilor și raportarea incidentelor pentru entitățile alimentare esențiale și importante ;

- **GDPR:** Regulamentul general privind protecția datelor, care stabilește reguli pentru protecția datelor cu caracter personal, protejează datele personale ale clienților și angajaților ;
- **ISO/IEC 27001:2022**: Un standard internațional pentru managementul securității informațiilor, cadrul pentru stabilirea unui sistem de management al securității informațiilor (SGSI) .
- **HACCP și ISO 22000:** Deși axată pe siguranța alimentară, securitatea cibernetică trebuie să se integreze cu aceste sisteme în care sunt implicate procesele digitale (monitorizarea temperaturii, trasabilitate).

1.7. Importanța educației și a conștientizării

- **Instruirea angajaților**: Educarea angajaților despre riscurile cibernetice și practicile sigure.
- **Simulări de atac**: Testarea răspunsului angajaților la amenințări.

1.8. Planuri de răspuns la incidente

- **Detectarea și analiza** incidentelor: Identificarea rapidă a activităților suspecte;
- **Izolarea și remedierea**: limitarea impactului incidentelor și restabilirea sistemelor;
- **Recuperare și învățare**: Analiza incidentelor pentru îmbunătățirea măsurilor de securitate.

Concluziile

Securitatea cibernetică este o componentă fundamentală a rezilienței sectorului alimentar. Prin înțelegerea riscurilor, implementarea controalelor de securitate stratificate și integrarea securității cibernetice cu sistemele de siguranță alimentară (de exemplu, HACCP), organizațiile pot asigura conformitatea, pot proteja operațiunile și pot menține încrederea consumatorilor într-un peisaj din ce în ce mai digital și reglementat.

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.

SECȚIUNEA 2. IDENTIFICAREA ȘI EVALUAREA RISCURILOR CIBERNETICE ÎN SECTORUL ALIMENTAR

2.1. Evaluarea riscurilor

2.1.1. Definiție

- **Evaluarea riscurilor** este procesul de identificare, analiză și evaluare a riscurilor cibernetice la care este expusă o organizație. Aceasta implică înțelegerea amenințărilor și vulnerabilităților, precum și a impactului potențial asupra activelor critice;

2.1.2. Importanța evaluării riscurilor în sectorul alimentar

- Evaluarea riscurilor în sectorul alimentar trebuie să ia în considerare convergența sistemelor IT și OT, în special în liniile de producție automatizate, sistemele de refrigerare și logistica. Dincolo de protejarea datelor, evaluările ar trebui să evalueze modul în care riscurile cibernetice afectează siguranța alimentară, conformitatea cu reglementările (de exemplu, ISO 22000) și continuitatea afacerii. Cartografierea vulnerabilităților sistemelor ICS/SCADA, a dispozitivelor IoT și a lanțurilor de aprovizionare digitale este esențială pentru a asigura atât securitatea cibernetică, cât și trasabilitatea alimentelor.

2.2. Pași în identificarea riscurilor

2.2.1. Identificarea activelor critice

- Primul pas este identificarea activelor critice ale organizației, cum ar fi sistemele de control industrial (ICS), datele clienților, sistemele de producție și lanțul de aprovizionare;

2.2.2. Identificarea amenințărilor și a vulnerabilităților

- Următorul pas este identificarea potențialelor amenințări (de exemplu, atacuri ransomware, breșe de date) și vulnerabilități (de exemplu, software învechit, lipsa autentificării cu mai mulți factori) care ar putea afecta activele critice. Riscul este probabilitatea ca o amenințare să exploateze o vulnerabilitate, înmulțită cu impactul posibil.

2.3. Metode de evaluare a riscurilor

2.3.1. Matricea riscurilor

- O matrice de risc este un instrument utilizat pentru a evalua riscurile, clasificându-le în funcție de probabilitatea lor de apariție și de impactul potențial. Acest lucru permite prioritizarea riscurilor și alocarea eficientă a resurselor pentru gestionarea acestora.

2.3.2. Instrumente și tehnici de evaluare

- Există diverse instrumente și tehnici de evaluare a riscurilor, inclusiv audituri de securitate, teste de penetrare, scanări de vulnerabilitate și evaluări ale conformității cu standardele de securitate. Atelierele de evaluare strategică pot ajuta la identificarea nevoilor critice de afaceri și a vulnerabilităților din rețele și sisteme informatice.

2.4. Exemple de riscuri specifice sectorului alimentar

2.4.1. Atacuri asupra lanțului de aprovizionare

- Atacurile asupra lanțului de aprovizionare digital pot compromite software-ul sau hardware-ul utilizat de furnizori, afectând astfel securitatea cibernetică a entităților din sectorul alimentar. Asigurarea securității lanțului de aprovizionare digital este o componentă-cheie a dispozițiilor Directivei NIS 2.

2.4.2. Compromiterea sistemelor de control industrial

- Sistemele de control industrial (ICS) sunt utilizate pentru a gestiona procesele de producție din sectorul alimentar. Compromiterea acestor sisteme poate duce la întreruperi ale producției, la calitatea produselor sau chiar la probleme de siguranță alimentară.

2.5. Amenințări cibernetice specifice alimentelor

2.5.1. Ransomware

- Atacatorii criptează datele unei organizații și cer o răscumpărare pentru a restabili accesul. Înainte de criptare, atacatorii exfiltrează date sensibile și amenință să le scurgă. Ransomware-ul HIVE a fost folosit în atacuri cibernetice pe mai multe platforme software, inclusiv Windows, Linux și ESXI Hypervisor.

2.5.2. Amenințări legate de date

- Acestea includ accesul neautorizat și scurgerile de date, în care infractorii cibernetici vizează sursele de date pentru acces neautorizat. Banii rămân cea mai frecventă motivație pentru astfel de atacuri.

2.5.3. Inginerie socială

- Păcălirea victimelor să deschidă documente, fișiere sau e-mailuri rău intenționate, oferind atacatorilor acces neautorizat la sisteme sau servicii. Phishing-ul (prin e-mail) sau smishing (prin mesaje text) sunt cele mai frecvente. Aproape 60% din penetrarea sistemelor de securitate include o componentă de inginerie socială

2.5.4. Amenințări la adresa disponibilității

- Atacuri care blochează accesul la date și servicii (DoS), afectând din ce în ce mai mult rețelele mobile și dispozitivele conectate.

2.5.5. Atacurile lanțului de aprovizionare

- Atacurile lanțului de aprovizionare pot compromite software-ul sau hardware-ul utilizat de furnizori, afectând astfel organizațiile din sectorul alimentar.

2.5.6. Compromiterea sistemelor de control industrial (ICS)

- Atacatorii preiau controlul asupra sistemelor care gestionează procesele de producție, ceea ce poate afecta siguranța alimentară.

2.5.7. Injectarea codului

- Atacatorii încearcă să extragă date, să fure acreditări, să preia controlul serverului web vizat sau să-și promoveze activitățile rău intenționate prin exploatarea vulnerabilităților aplicațiilor web.

2.5.8. Exploit-uri de tip drive-by

- Distribuția de malware prin exploit-uri drive-by se concentrează aproape în întregime pe compromiterea site-urilor web legitime.

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.

SECȚIUNEA 3. MĂSURI DE SECURITATE CIBERNETICĂ

Pentru a proteja organizațiile din sectorul alimentar împotriva amenințărilor cibernetice, este esențial să se pună în aplicare o combinație de măsuri tehnice, organizatorice și procedurale. Iată o defalcare a principalelor măsuri de securitate cibernetică:

3.1. Evaluarea dimensiunii economice

3.1.1. Firewall-uri, sisteme de detectare a intruziunilor (IDS) și sisteme de prevenire a intruziunilor (IPS)

- **Firewall-uri**:
  - **Funcție**: Blochează traficul nesolicitat și potențial rău intenționat între rețele;
  - **Beneficii**: Protejează rețelele interne de acces neautorizat și atacuri externe;
  - **Exemplu**: Configurarea unui firewall pentru a permite numai traficul legitim către și dinspre rețeaua organizației.
- **Sisteme de detectare a intruziunilor (IDS):**
  - **Caracteristică**: Monitorizează rețeaua pentru activități suspecte și generează alerte;
  - **Beneficii**: Detectează tentativele de atac sau comportamentele anormale.
- **Sisteme de prevenire a intruziunilor (IPS):**
  - **Caracteristică**: Blochează automat activitățile rău intenționate detectate.

3.1.2. Actualizări regulate și gestionarea patch-urilor

- **Actualizări software**:
  - **Caracteristică**: Remediază vulnerabilitățile cunoscute în sistemele de operare, aplicații și firmware.
- **Gestionarea patch-urilor**:
  - **Funcție**: Gestionarea sistematică și aplicarea patch-urilor de securitate.

3.2. Managementul accesului

3.2.1. Autentificarea cu mai mulți factori (MFA)

- **Caracteristică**: Necesită mai multe forme de verificare pentru a accesa sistemele (de exemplu, parolă + cod trimis pe telefon).
- **Beneficii**: Reduce riscul de acces neautorizat chiar dacă parola este compromisă.
- **Exemplu**: Implementarea MFA pentru accesul la sisteme critice și date sensibile.

3.2.2. Controlul accesului bazat pe roluri (RBAC)

- **Caracteristică**: Limitează accesul la resurse în funcție de rolul utilizatorului în organizație.
- **Beneficii**: Asigură că fiecare utilizator are acces doar la resursele necesare pentru a-și îndeplini sarcinile.
- **Exemplu**: Un angajat din producție are acces doar la sisteme de control industrial, nu și la date financiare.

3.3. Protecția datelor

3.3.1. Criptarea datelor atât în repaus, cât și în tranzit

- **Criptare în repaus**:
  - **Funcție**: Protejează datele stocate pe servere, dispozitive de stocare sau în cloud.
- **Criptare în tranzit**:
  - **Funcție**: Protejează datele transmise între sisteme sau prin internet.
  - **Beneficii**: Previne interceptarea și citirea datelor de către atacatori.
- **Exemplu**: utilizarea HTTPS pentru a comunica cu site-uri web și API-uri.

3.3.2. Copii de rezervă periodice și planuri de recuperare a datelor

- **Copii de rezervă** regulate:
  - **Funcție**: Crearea de copii de rezervă ale datelor critice la intervale regulate.
  - **Beneficii**: Asigură recuperarea datelor în caz de pierdere sau ștergere accidentală.
- **Planuri de recuperare a datelor**:
  - **Funcționalitate**: Definește pașii pentru restaurarea datelor și sistemelor după un incident.
  - **Beneficii**: Minimizează timpul de nefuncționare și pierderea datelor.
- **Exemplu**: Efectuarea de copii de rezervă zilnice și testarea periodică a procesului de recuperare.

3.4. Securitatea sistemelor de control industrial (ICS)

3.4.1. Izolarea rețelelor industriale (air-gapping)

- **Funcție**: Asigurarea segmentării între mediile OT și IT folosind firewall-uri, DMZ și gateway-uri unidirecționale, acolo unde este cazul. Evitarea bazării exclusiv pe spațiul fizic de aer, deoarece multe medii de procesare a alimentelor necesită schimb de date (de exemplu, între ERP și ICS). Aplicarea controalelor stricte de acces și monitorizare între zone.
- **Beneficii**: Reduce riscul de atacuri cibernetice asupra sistemelor de control industrial.
- **Exemplu**: Utilizarea rețelelor dedicate pentru echipamente de producție fără conexiune la internet.

3.4.2. Monitorizarea continuă a sistemelor ICS

- **Funcție**: Monitorizarea în timp real a activității sistemelor de control industrial pentru detectarea anomaliilor.
- **Beneficii**: Permite identificarea rapidă a activităților suspecte sau a tentativelor de atac.
- **Exemplu**: Implementarea soluțiilor specializate de monitorizare pentru ICS, care detectează modificări neautorizate ale parametrilor de producție.

3.5. Măsuri suplimentare recomandate

3.5.1. Formarea și sensibilizarea angajaților

- **Funcție**: Dezvoltarea programelor de instruire personalizate pentru lucrătorii de pe linia de producție, personalul din depozit, personalul QA/QC și echipele IT. Pentru operatorii

ICS/OT, integrarea igienei digitale în briefing-urile privind siguranța alimentară (de exemplu, impactul dispozitivelor USB neautorizate sau al configurațiilor PLC nesigure). Includerea de simulări ale amenințărilor reale, cum ar fi alerte de întreținere falsificate sau inginerie socială care vizează supraveghetorii fabricii.

- **Beneficii**: Reduce riscul de eroare umană care poate duce la breșe de securitate
- **Exemplu**: instruiri regulate privind phishingul, gestionarea parolelor și securitatea dispozitivelor mobile.

3.5.2. Planuri de răspuns la incidente

- **Funcție**: Definirea pașilor de urmat în cazul unui incident cibernetic.
- **Beneficii**: Asigură un răspuns rapid și eficient pentru a minimiza impactul.
- **Exemplu**: Creați un plan care include identificarea, reținerea, remedierea și recuperarea după un incident.

3.5.3. Colaborarea cu partenerii și furnizorii

- **Funcție**: Asigurarea faptului că partenerii și furnizorii respectă standarde înalte de securitate.
- **Beneficii**: Reduce riscurile lanțului de aprovizionare.
- **Exemplu**: evaluarea securității cibernetice a furnizorilor și includerea cerințelor de securitate în contracte.

Concluzie

Implementarea acestor măsuri de securitate cibernetică este esențială pentru a proteja organizațiile de afaceri alimentare de amenințările cibernetice. Prin combinarea soluțiilor tehnice, a politicilor clare și a educației angajaților, organizațiile pot reduce riscurile, pot asigura conformitatea cu reglementările și pot menține încrederea clienților și partenerilor.

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.

SECȚIUNEA 4. RESPECTAREA NIS 2 ȘI A ALTOR REGLEMENTĂRI

Pentru organizațiile din industria alimentară, respectarea reglementărilor de securitate cibernetică este esențială pentru a minimiza riscurile, a proteja datele sensibile și a evita sancțiunile.

4.1. Cerințe ale Directivei NIS 2

4.1.1. Obligațiile organizațiilor din sectorul alimentar

➲ **Ce este NIS 2?**

- **NIS 2** (Directiva UE privind securitatea rețelelor și a sistemelor informatice) este o actualizare a Directivei NIS, care extinde domeniul de aplicare și introduce cerințe mai stricte pentru securitatea cibernetică;

➲ **Cine este afectat?**

- Entitățile esențiale includ companii mari din domenii precum energie, transporturi, sănătate sau companii considerate mari, pe baza cifrei de afaceri, care furnizează servicii esențiale;
- Printre entitățile importante se numără organizațiile mijlocii din domenii precum producția, curieratul sau distribuția de alimente, care sunt esențiale la nivel de țară, dar nu au același grad de vulnerabilitate;
- Directiva vizează întreprinderile alimentare care își desfășoară activitatea exclusiv în domeniul logisticii, distribuției angro și producției și prelucrării industriale la scară largă, cu o cotă de piață semnificativă la nivel național

➲ **Obligații cheie:**

- **Implementarea măsurilor de securitate** adecvate:
  - Organizațiile trebuie să adopte măsuri tehnice și organizatorice pentru a gestiona riscurile cibernetice.
- **Managementul riscului**:
  - Evaluarea periodică a riscurilor și implementarea măsurilor de reducere a riscurilor.
- **Notificarea incidentelor**:
  - Întreprinderile trebuie să aplice o gestionare eficace a riscurilor și să raporteze incidentele cibernetice grave sau semnificative autorităților naționale competente.
- **Cooperarea cu** autoritățile:
  - Colaborarea cu autoritățile naționale și europene pentru îmbunătățirea securității cibernetice;
  - Entitățile iau măsuri tehnice, operaționale și organizatorice adecvate pentru a gestiona riscurile care amenință securitatea sistemelor informatice utilizate pentru operațiunile lor.

4.1.2. Raportarea incidentelor și gestionarea riscurilor

➲ **Raportarea incidentelor:**

- Organizațiile trebuie să raporteze rapid și fără întârzieri nejustificate orice incident de securitate cibernetică cu impact semnificativ;

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.

- Organizațiile clasificate ca esențiale sau importante conform NIS2 (pe baza dimensiunii și relevanței) trebuie să raporteze incidentele majore după cum urmează:
  - Notificare inițială: în termen de 24 de ore prin intermediul platformei DNSC NIS2@RO;
  - Raport tehnic detaliat: în termen de 72 de ore;
  - Raport final de remediere: în termen de 30 de zile calendaristice;
- Incidentele includ: compromiterea sistemelor ICS/SCADA, întreruperea trasabilității alimentelor, exfiltrarea datelor sau DoS care afectează producția.
- **Exemple de incidente raportabile**: atacuri ransomware, încălcări ale datelor, întreruperi majore ale sistemelor de producție.

➲ **Managementul riscului:**

- Implementarea unui cadru de management al riscului care include:
  - Identificarea și evaluarea riscurilor;
  - Implementarea măsurilor de prevenire și protecție;
  - Monitorizarea continuă și îmbunătățirea posturii de securitate.

Directiva NIS 2 abordează securitatea lanțurilor de aprovizionare și a relațiilor cu furnizorii, solicitând întreprinderilor să abordeze riscurile de securitate cibernetică în lanțurile de aprovizionare.

4.2. GDPR și protecția datelor

Directiva NIS2 stabilește un cadru juridic unificat pentru a sprijini securitatea cibernetică în 18 sectoare critice din întreaga UE.

În plus față de cerințele NIS 2, organizațiile din sectorul alimentar trebuie să respecte și Regulamentul general privind protecția datelor (GDPR) pentru a proteja datele personale ale clienților și angajaților.

4.2.1. Ce este GDPR

➲ **GDPR** (Regulamentul General privind Protecția Datelor) este un regulament european care stabilește reguli stricte pentru protecția datelor cu caracter personal;

➲ **Aplicabilitate**: Se aplică tuturor organizațiilor care prelucrează date cu caracter personal ale cetățenilor UE.

4.2.2. Cum să protejați datele cu caracter personal ale clienților și angajaților

➲ **Minimizarea datelor:**

- Colectarea și prelucrarea numai a datelor cu caracter personal necesare.

➲ **Consimțământ:**

- Obținerea consimțământului explicit al persoanelor înainte de prelucrarea datelor acestora.

➲ **Criptarea datelor**:

- Protejați datele personale cu criptare atât în repaus, cât și în tranzit.

➲ **Managementul accesului**:

- Limitarea accesului la datele cu caracter personal doar la persoanele autorizate.

➲ **Notificarea încălcărilor securității**:

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.

- Raportarea oricărei încălcări a datelor cu caracter personal către autoritățile de protecție a datelor în termen de 72 de ore.

➲ **Politici de confidențialitate**:

- Asigurarea faptului că atât clienții, cât și angajații sunt informați despre modul în care sunt procesate datele lor.

4.3. Standarde internaționale de securitate cibernetică

4.3.1. ISO/IEC 27001

➲ **Ce este ISO/IEC 27001:**

- Un standard internațional care oferă un cadru pentru implementarea unui sistem de management al securității informațiilor (ISMS).

➲ **Beneficii**:

- **Abordare** sistematică: Ajută organizațiile să identifice, să evalueze și să gestioneze riscurile de securitate a informațiilor.
- **Conformitate**: demonstrează conformitatea cu reglementările precum GDPR și NIS 2.
- **Încredere îmbunătățită**: Crește încrederea clienților și a partenerilor de afaceri.

➲ **Elemente cheie**:

- **Evaluarea riscurilor**: Identificarea riscurilor pentru activele informaționale.
- **Politici și proceduri**: Dezvoltarea politicilor de securitate a informațiilor.
- **Monitorizare și audit:** Revizuirea periodică a sistemului pentru a asigura eficiența.

4.3.2. Vechile standarde relevante:

Organizațiile pot utiliza standarde internaționale de securitate cibernetică, cum ar fi ISO/IEC 27001, pentru a stabili, implementa, menține și îmbunătăți continuu un sistem de management al securității informațiilor (ISMS).

Aceste standarde oferă un cadru de bune practici pentru gestionarea securității informațiilor și pot ajuta organizațiile să demonstreze conformitatea cu cerințele legale și de reglementare.

Directiva impune fiecărui stat membru să adopte o strategie națională de securitate cibernetică, inclusiv politici privind securitatea lanțului de aprovizionare, gestionarea vulnerabilităților și educația și conștientizarea securității cibernetice.

➲ **ISO/IEC 27002:** Oferă linii directoare și cele mai bune practici pentru implementarea controalelor de securitate a informațiilor

➲ **Cadrul de securitate cibernetică NIST**: Un cadru dezvoltat de Institutul Național de Standarde și Tehnologie (NIST) din SUA care oferă recomandări pentru gestionarea riscurilor cibernetice;

➲ **PCI DSS (Payment Card Industry Data Security Standard):** Obligatoriu pentru organizațiile care procesează plăți cu cardul, pentru a proteja datele cardurilor de credit;

➲ **IEC 62443:** Standard pentru siguranța sistemelor de control industrial (ICS), relevant pentru sectorul alimentar.

4.4. Asigurarea conformității

4.4.1. Evaluarea stării

- Efectuarea unui audit pentru a evalua nivelul de conformitate cu NIS 2, GDPR și alte standarde relevante;
- Identificați lacunele și dezvoltați un plan de acțiune pentru a le remedia.

4.4.2. Punerea în aplicare a măsurilor de securitate

- Adoptarea de măsuri tehnice (de exemplu, criptare, firewall-uri) și organizatorice (politici, proceduri);
- Asigurarea faptului că toate sistemele și software-ul sunt actualizate și corectate;

4.4.3. Formarea angajaților

- Organizarea de cursuri de formare periodice pentru a crește gradul de conștientizare cu privire la securitatea cibernetică și protecția datelor.

4.4.4. Monitorizare și revizuire continuă

- Monitorizarea activității rețelelor și sistemelor pentru a detecta și a răspunde rapid la amenințări;
- Revizuirea periodică a politicilor și procedurilor pentru a se asigura că acestea rămân eficiente și conforme.

4.5. Documentare și monitorizare continuă

4.5.1. Raportul final de calificare

- **Documentație detaliată:** Pregătirea unui raport final care să documenteze întregul proces de evaluare și calificare, inclusiv toți pașii și concluziile relevante;
- **Arhivarea documentelor:** Arhivarea raportului și a tuturor documentelor justificative pentru referințe ulterioare și pentru eventuale inspecții sau audituri.

4.5.2. Monitorizarea continuă

- **Revizuiri periodice:** Stabilirea unui program de revizuiri periodice pentru a actualiza evaluările și a asigura conformitatea continuă cu Directiva NIS2.
- **Actualizarea informațiilor:** Menținerea la zi a informațiilor despre dimensiunea economică, structura organizațională și conformitatea entității.

Această etapă finală de clasificare asigură că toate entitățile relevante din industria alimentară sunt identificate corect și în conformitate cu cerințele Directivei NIS2. Procesul detaliat de evaluare și calificare contribuie la securitatea și reziliența infrastructurilor critice, protejând astfel securitatea alimentară și sănătatea publică.

Cerința OUG 155/2024 din România/ Legea de modificare a cerințelor Legii bulgare privind securitatea cibernetică	Fundamentele cibernetice	ISO/IEC 27001:2022	Funcția NIST CSF	Comentariu
Măsuri de securitate proporționale	Toate nivelurile CyFUN	A.5, A.6, A.8	Protejare (PR)	Adaptarea la scorul de risc DNSC/BGMEG
Raportarea unui incident (art. 16-18, conform OUG 155/2024)	RS.CO, RS. LOR	A.16, A.17	Răspunde (RS)	24h/72h/30d

Evaluarea riscurilor și autoanaliza	ID.RA, ID.RM	A.6, A.15	Identificare (ID)	Formular DNSC/BGMEG, evaluare anuală
Audit periodic	PR. PT-1, ID.RA-3	A.9, A.10	Protejare (PR)	Minim pentru entitate importantă
Clasificarea entităților (scor DNSC/BGMEG)	–	–	–	Anexa 2 Ordinul DNSC 2024/ Cadrul de reglementare subsidiar după adoptarea Legii bulgare privind modificările și completările la Legea privind securitatea cibernetică

Concluzie:

Conformitatea cu Directiva NIS 2, GDPR și alte standarde de securitate cibernetică este esențială pentru organizațiile de afaceri alimentare. Prin implementarea măsurilor de securitate adecvate, gestionarea riscurilor și conformitatea cu reglementările, organizațiile pot proteja activele critice, pot asigura confidențialitatea datelor și pot menține încrederea clienților și partenerilor.

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.

SECȚIUNEA 5. SECURITATEA LANȚULUI DE APROVIZIONARE

5.1. Riscuri cibernetice în lanțul de aprovizionare digital

5.1.1. Vulnerabilitățile partenerilor și furnizorilor.

- Efectuarea de evaluări periodice ale riscurilor de securitate cibernetică pentru furnizori folosind o listă de verificare standardizată bazată pe ISO 27036 și ISO 28000.

  Evaluare la:

  - Politica de gestionare a patch-urilor furnizorului;
  - Acces la sistemele dumneavoastră (VPN, API-uri);
  - Capacitățile lor de raportare a incidentelor;
  - Respectarea obligațiilor DNSC (dacă se află în România).

Includerea clauzelor de securitate în contracte, definirea de responsabilități comune și solicitarea asigurării cibernetice pentru partenerii critici.

5.2. Măsuri de securitate a lanțului de aprovizionare

Pentru a minimiza întreruperile lanțului de aprovizionare, companiile trebuie să adapteze dinamic modurile de transport, folosind informații în timp real. Gestionarea automată a expedierilor și procesele de expediere, colaborarea în cloud și documentația de expediere standardizată pot ajuta la compensarea acestor riscuri.

5.2.1. Evaluarea securității partenerilor.

- Amenințările cibernetice reprezintă un risc major pentru securitatea lanțului de aprovizionare, deoarece rețelele IT și dispozitivele conectate pot crea portaluri pentru infractorii cibernetici. Peste 80% din incidentele cibernetice ale unei companii provin din compromiterea furnizorilor. Astfel, este important să alegeți soluții software cu funcții securizate de securitate cibernetică;
- O strategie organizațională și programatică care implică activități de evaluare și gestionare a riscurilor de securitate cibernetică, inclusiv riscuri specifice lanțului de aprovizionare, este esențială.
- ISO 28000 este un standard de sistem de management al siguranței, aplicabil în toate organizațiile care fac parte dintr-un lanț de aprovizionare, oferind posibilitatea de a efectua evaluări de risc și de a aplica metode adecvate pentru a menține aceste riscuri sub control.

5.2.2. Contracte și cerințe de securitate pentru furnizori

- Implementarea unui sistem de management al securității contribuie la creșterea nivelului de conștientizare a securității la toate nivelurile organizației [3]. Standardele de securitate deja implementate pot fi integrate într-un singur sistem complet, în conformitate cu ISO 28000.

5.3. Colaborare și schimb de informații

Colaborarea la securitatea rețelei, dispozitive și programe poate ajuta la identificarea și atenuarea amenințărilor. De asemenea, investițiile în formarea angajaților în domeniul securității sunt esențiale.

Pentru a evalua securitatea partenerilor din lanțul de aprovizionare, pot fi utilizate următoarele metode:

5.3.1. Monitorizarea performanței furnizorilor.

- Producătorii pot identifica problemele când și unde apar, pot evalua gravitatea acestora, pot oferi furnizorilor feedback informat, pot lucra împreună pentru a găsi soluții și pot decide dacă problemele de performanță sunt un motiv pentru parteneriat;

5.3.2. Măsurarea performanței

- Producătorii măsoară performanța furnizorilor în mai multe moduri, inclusiv respectarea contractelor, performanța operațională (calitatea muncii, termenele de livrare, livrarea la timp, livrarea completă), procesele de afaceri (prevenirea defectelor, inspecțiile, conformitatea cu reglementările) și situația financiară (risc de faliment, lichiditate, profitabilitate);

5.3.3. Utilizarea unui tabel de tip scorecard KPI

- Măsurile standard permit companiilor să facă comparații între furnizori. Monitorizarea performanței funcționează cel mai bine atunci când este continuă, cu revizuiri și verificări regulate ale furnizorilor;

5.3.4. Evaluarea riscurilor lanțului de aprovizionare

- Identificarea riscurilor potențiale pentru lanțul de aprovizionare, fie că acestea vin sub formă de modificări ale cererii (din cauza inflației), fiabilității furnizorilor (ca urmare a Covid), întreruperi ale transportului (Canalul Suez), modificări de reglementare (Brexit) sau dezastre naturale (schimbări climatice);

5.3.5. Colectarea informațiilor

- Producătorii colectează informații despre performanța furnizorilor lor pentru a controla costurile, a reduce riscurile și a-i responsabiliza pentru livrarea produselor de calitate la timp. Aceste informații includ, de asemenea, date privind respectarea de către furnizori a legislației privind siguranța lucrătorilor, drepturile omului și mediul, menționând orice încălcări actuale sau trecute. Unele aplicații SCM automatizează această captură de date și emit alerte de neconformitate;

5.3.5. Revizuirea obiectivelor stabilite

- Companiile măsoară progresul transparenței lanțului lor de aprovizionare prin revizuirea obiectivelor stabilite, identificarea îmbunătățirilor și discutarea obiectivelor pe care nu le-au atins (și de ce). Colaborarea strânsă cu furnizorii este esențială;

5.3.5. Certificarea ISO 28000

- Certificarea ISO 28000 oferă un cadru pentru organizațiile care operează sau se bazează pe orice element al lanțului de aprovizionare pentru a evalua și implementa controale pentru a reduce riscurile de securitate.

SECȚIUNEA 6. RĂSPUNS LA INCIDENTE CIBERNETICE

6.1. Plan de răspuns la incidente cibernetice

Un plan de răspuns la incidente este un manual de acțiune pentru gestionarea incidentelor de securitate. Asigură un răspuns rapid și eficient, minimizând impactul unei breșe de securitate. Un plan bine definit vă permite să identificați problema, să minimizați daunele și să reduceți costul unui atac.

6.2. Pași pentru gestionarea incidentelor

Înțelegerea fazelor de gestionare a incidentelor este esențială pentru un răspuns eficient la securitatea cibernetică.

6.2.1. Detectarea și analiza incidentelor:

- După detectarea incidentului și a sursei acestuia, trebuie să limitați daunele.

6.2.2. Izolare și remediere:

- Acest lucru poate implica dezactivarea accesului la rețea pentru computerele infectate și instalarea de soluții de securitate suplimentare. De asemenea, poate fi necesar să resetați parolele sau să blocați conturile persoanelor care ar fi putut cauza incidentul.

6.2.3. Recuperarea și învățarea din incidente:

- Urmează restaurarea serviciilor, validarea și testarea sistemului. Orice componente compromise ar trebui verificate, iar conturile care au permis intruziune ar trebui eliminate sau blocate.

6.3. Exemple de incidente cibernetice în sectorul alimentar:

Deși nu există studii de caz specifice privind incidentele cibernetice din sectorul alimentar, putem învăța lecții valoroase din incidentele de securitate cibernetică în general:

- **Importanța securității cibernetice:** Adoptarea muncii de la distanță a accelerat digitalizarea, evidențiind nevoia de securitate cibernetică.
- **Costurile incidentelor de securitate:** Incidentele de securitate pot duce la pierderi financiare semnificative, inclusiv amenzi substanțiale, costuri de remediere și pierderea oportunităților de afaceri. Costul mediu al unei breșe de date a fost de 3,35 milioane de dolari în 2020, în creștere cu 9,8% față de anul precedent.
- **Cauzele incidentelor de securitate:** Incidentele de securitate pot fi cauzate de factori precum parole nesigure, procese necorespunzătoare, vulnerabilități ale sistemului, lipsa actualizărilor, atacuri asupra partenerilor, malware și erori umane.
- **Impactul incidentelor de securitate:** Incidentele de securitate pot afecta orice tip de utilizator, de la persoane fizice la companii multinaționale, ducând la compromiterea identității și reputației, precum și la furtul de bani.
- **Măsuri de prevenire:** Implementarea tehnologiilor de automatizare în cadrul serviciilor de securitate cibernetică poate reduce semnificativ costurile unei breșe de date și timpul de răspuns; Pregătirea pentru răspunsul la incidente prin exerciții și simulări poate contribui la economii semnificative.

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.

- **Nevoia unui sistem de securitate proactiv:** Optarea pentru un sistem de securitate proactiv, cum ar fi un centru de operațiuni de securitate (SOC), poate îmbunătăți capacitățile de monitorizare și răspuns la incidente.
- **Cartografierea nivelului de securitate cibernetică:** Echipa DNSC își propune să cartografieze nivelul de securitate cibernetică pentru entitățile din sectorul alimentar.
- **Amenzi pentru nerespectarea cerințelor de securitate**.

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.

SECȚIUNEA 7. EDUCAREA ȘI CONȘTIENTIZAREA ANGAJAȚILOR

7.1. Rolul angajaților în securitatea cibernetică

Angajații joacă un rol esențial în menținerea securității cibernetice a unei organizații. Aceștia trebuie să fie conștienți de potențialele amenințări cibernetice și să ia măsurile de precauție necesare pentru a proteja datele sensibile. Aceasta include vigilența atunci când accesați e-mailuri sau utilizați dispozitive mobile și evitați să faceți clic pe link-uri sau atașamente suspecte. Educarea și instruirea angajaților cu privire la problemele de securitate cibernetică poate reduce semnificativ probabilitatea ca aceștia să cadă în capcana atacurilor de phishing. Astfel, angajații pot deveni o primă linie de apărare împotriva atacurilor cibernetice, îmbunătățind securitatea generală a organizației.

7.2. Programe de formare și conștientizare:

7.2.1. **Dezvoltarea** unui program eficient

- Proiectarea unor programe de conștientizare aliniate cu rolurile:
  - IT și InfoSec: răspuns la incidente, informații despre amenințări, monitorizare SIEM ;
  - Operatori OT/ICS: utilizarea securizată a dispozitivului, igiena accesului de la distanță;
  - Management: asumarea riscurilor, luarea deciziilor sub presiune Cibernetică;
  - QA și HACCP: impactul amenințărilor cibernetice asupra siguranței alimentare și a proceselor de retragere.
- Trebuie să acopere o gamă largă de subiecte și tehnici pentru a oferi angajaților puterea de a lua deciziile corecte.
- Un astfel de program trebuie să fie un proces formalizat, conceput pentru a crește abilitățile angajaților și a reduce riscul unei posibile breșe de securitate.
- Utilizarea de simulări periodice și platforme de învățare adaptivă pentru o retenție maximă.

7.2.2. **Subiecte esențiale:** phishing, gestionarea parolelor, securitatea dispozitivelor mobile

- Phishing: instruirea ar trebui să includă recomandări esențiale pentru a recunoaște și a evita atacurile de phishing. Simulările și testele periodice pot crește înțelegerea de către angajați a tipurilor și impactului atacurilor cibernetice.
- Managementul parolelor: Angajații trebuie să fie instruiți cu privire la importanța utilizării parolelor puternice și a gestionării lor în siguranță.
- Securitatea dispozitivelor mobile: Instruirea ar trebui să acopere măsurile de precauție necesare pentru a proteja datele sensibile atunci când utilizați dispozitive mobile.

7.3. Simulări de atacuri cibernetice:

- Simulările de atacuri cibernetice efectuate periodic sunt o modalitate eficientă de a testa răspunsul angajaților la amenințări și de a identifica zonele care necesită îmbunătățiri în timp util.
- Aceste simulări ajută la completarea cunoștințelor teoretice despre phishing și alte tipuri de atacuri cibernetice.
- Prin testarea regulată a cunoștințelor angajaților, organizațiile pot îmbunătăți înțelegerea și își pot consolida apărarea împotriva amenințărilor cibernetice.

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.

SECȚIUNEA 8. MONITORIZARE ȘI ÎMBUNĂTĂȚIRE CONTINUĂ

8.1. Importanța monitorizării continue

Monitorizarea continuă este un element esențial al strategiilor de securitate cibernetică, în special în sectorul alimentar, unde sistemele de producție, lanțul de aprovizionare și datele sensibile sunt expuse unor riscuri cibernetice semnificative. Aceasta implică observarea și analizarea constantă a rețelelor, sistemelor și activităților pentru a detecta și a răspunde rapid la potențialele amenințări. Iată de ce este atât de important.

8.1.1. Detectarea timpurie a amenințărilor: Monitorizarea continuă permite identificarea rapidă a activităților suspecte sau a tentativelor de atac înainte ca acestea să provoace daune semnificative (detectarea unui atac de phishing în faza inițială, înainte ca angajații să facă clic pe link-uri rău intenționate; identificarea comportamentelor anormale de rețea care ar putea indica un **atac ransomware** sau **DDoS**).

8.1.2. Răspuns rapid la incidente: monitorizarea continuă oferă informații în timp real, permițând echipei de securitate să acționeze imediat pentru a limita impactul unui incident (închiderea automată a unui port de rețea care este scanat de un atacator; izolarea unui dispozitiv infectat pentru a preveni răspândirea malware-ului).

8.1.3. Reducerea la minimum a timpilor de nefuncționare: În sectorul alimentar, întreruperile producției sau distribuției pot avea consecințe financiare grave. Monitorizarea continuă ajută la prevenirea sau limitarea acestor întreruperi (detectarea și remedierea rapidă a unei defecțiuni într-un sistem de control industrial (ICS) care ar putea duce la o oprire a producției).

8.1.4. Protecția datelor sensibile: Implementarea sistemelor de prevenire a pierderii datelor (DLP), stocare criptată și înregistrarea accesului pentru active sensibile, cum ar fi contracte cu furnizorii, baze de date ale clienților și formule de rețete. Utilizarea instrumentelor de detectare a anomaliilor pentru a identifica încercările de exfiltrare sau descărcările neautorizate.

8.1.5. Conformitatea cu reglementările: Multe reglementări, cum ar fi **NIS 2** și **GDPR,** impun organizațiilor să monitorizeze activitatea sistemului și să raporteze incidentele în scurt timp. (Raportarea unui incident cibernetic către autoritățile competente în termen de 24 de ore, conform cerințelor NIS 2; monitorizarea accesului la datele cu caracter personal pentru a asigura conformitatea cu GDPR).

8.1.6. Identificarea vulnerabilităților: Monitorizarea continuă ajută la identificarea vulnerabilităților din sisteme și rețele înainte ca acestea să fie exploatate de atacatori (detectarea software-ului învechit care ar putea fi exploatat de un atacator; identificarea unei configurații slabe a firewall-ului care permite accesul neautorizat).

8.1.7. Procesul de consolidare și optimizare a măsurilor și practicilor de securitate: Prin analiza continuă a datelor de securitate, organizațiile pot identifica tendințe și modele care le permit să-și îmbunătățească strategiile de securitate. (Identificarea unui tip de atac care apare frecvent și implementarea unor măsuri specifice pentru a-l preveni; optimizarea politicilor de securitate pe baza datelor colectate).

8.2. Instrumente de monitorizare a securității:

- **Sisteme de detectare și prevenire a atacurilor (IDS/IPS):** care vizează monitorizarea traficului de rețea pentru a detecta și bloca activități suspecte sau atacuri cibernetice;
- **Soluții de monitorizare a securității rețelei:** utilizarea inteligenței artificiale și a învățării automate pentru a identifica comportamentele anormale ale rețelei;
- **Instrumente de gestionare a vulnerabilităților:** scanarea sistemelor și rețelelor pentru a identifica vulnerabilitățile și a recomanda remedieri;
- **Sisteme de management al informațiilor și evenimentelor de securitate (SIEM):** centralizarea și analizarea datelor din mai multe surse pentru a detecta și a răspunde amenințărilor în timp real;
- **Instrumente de securitate a dispozitivelor IT**: protejarea dispozitivelor IT (cum ar fi cele utilizate în producția și distribuția alimentelor) împotriva atacurilor cibernetice;
- **Soluții de securitate a datelor:** monitorizarea și protejarea datelor sensibile împotriva accesului sau pierderii neautorizate;
- **Instrumente de testare a penetrării:** simularea atacurilor cibernetice pentru a identifica punctele slabe ale sistemului;
- **Soluții de securitate în cloud**: monitorizarea și protejarea datelor și aplicațiilor găzduite în cloud;
- **Instrumente de conformitate și audit:** asigurarea conformității cu standardele de securitate (cum ar fi GDPR, ISO 27001) și facilitarea auditurilor de securitate**;**
- **Sisteme de răspuns la incidente:** identificarea și remedierea rapidă a incidentelor de securitate;
- **Instrumente de securitate a lanțului de aprovizionare:** monitorizarea și protejarea lanțului de aprovizionare împotriva riscurilor cibernetice;
- Soluții de securitate pentru SCADA/ICS: protecția sistemelor de control industrial (SCADA) și a sistemelor de operare tehnologice (OT) utilizate în industria alimentară;
- **Soluții de securitate a aplicațiilor web**: identificarea vulnerabilităților din aplicațiile web utilizate pentru gestionarea comenzilor, logistică sau servicii pentru clienți;
- **Instrumente de formare și conștientizare a angajaților:** educarea angajaților cu privire la riscurile cibernetice și cele mai bune practici de securitate.

8.3. Audituri și evaluări periodice:

8.3.1. Educația și conștientizarea angajaților:

- Angajații joacă un rol crucial în menținerea securității cibernetice a unei organizații. Acestea trebuie să fie conștiente de potențialele amenințări cibernetice și să ia măsurile de precauție necesare pentru a proteja datele sensibile;
- Aceasta include vigilența atunci când accesați e-mailuri sau utilizați dispozitive mobile și evitați să faceți clic pe link-uri sau atașamente suspecte. Educarea și instruirea angajaților cu privire la problemele de securitate cibernetică poate reduce semnificativ probabilitatea ca aceștia să cadă în capcana atacurilor de phishing. Astfel, angajații pot deveni o primă linie de apărare împotriva atacurilor cibernetice, îmbunătățind securitatea generală a organizației.

8.3.2. Dezvoltarea unui program eficient

Un program eficient de instruire în domeniul securității cibernetice este esențial pentru a schimba comportamentele angajaților și a-i educa cu privire la riscurile cibernetice și cele mai bune practici. Ar trebui să acopere o gamă largă de subiecte și tehnici pentru a le permite angajaților să ia deciziile corecte. Un astfel de program ar trebui să fie un proces formalizat, conceput pentru a îmbunătăți abilitățile angajaților și a reduce riscul unei potențiale breșe de securitate.

8.3.3. Principalele subiecte care trebuie discutate

- Phishing ce: Instruirea ar trebui să includă sfaturi esențiale pentru recunoașterea și evitarea atacurilor de phishing. Simulările și testarea periodică pot crește înțelegerea de către angajați a tipurilor și impactului atacurilor cibernetice;
- Managementul parolelor: Angajații trebuie să fie instruiți cu privire la importanța utilizării parolelor puternice și a gestionării lor în siguranță;
- Securitatea dispozitivelor mobile: Instruirea ar trebui să acopere măsurile de precauție necesare pentru a proteja datele sensibile atunci când utilizați dispozitive mobile;
- Simulările de atacuri cibernetice sunt o modalitate eficientă de a testa răspunsul angajaților la amenințări și de a identifica zonele care necesită îmbunătățiri;
- Aceste simulări ajută la completarea cunoștințelor teoretice despre phishing și alte tipuri de atacuri cibernetice;
- Prin testarea regulată a cunoștințelor angajaților, organizațiile pot îmbunătăți înțelegerea și își pot consolida apărarea împotriva amenințărilor cibernetice.

SECȚIUNEA 9: STUDII DE CAZ ȘI EXEMPLE PRACTICE

9.1. Incidente cibernetice în sectorul alimentar

- Echipa DNSC din România își propune să cartografieze nivelul de securitate cibernetică pentru entitățile din sectorul alimentar. Sectorul energetic din România a reprezentat 31% din toate atacurile cibernetice în 2023, urmat de sectorul transporturilor cu 22% și serviciile guvernamentale cu 19%;
- În România, incidența zilnică a atacurilor cibernetice este de 20.000-30.000. Principalele industrii vizate sunt industria farmaceutică, administrația publică, energia, comerțul cu amănuntul și transporturile; În Bulgaria, în 2024, Echipa Națională de Răspuns la Incidente de Securitate Informatică a remarcat o complicație continuă a situației cibernetice din țară, cu 8951 de semnale înregistrate. Dintre acestea, 3775 au fost înregistrate ca incidente, conform taxonomiei Agenției Europene de Securitate Cibernetică – ENISA. Cele mai frecvente cauze ale incidentelor rămân răspândirea codului rău intenționat (66%) și frauda (phishing) (31%). Echipa Națională de Răspuns la Incidente de Securitate Informatică a trimis 6 206 recomandări și instrucțiuni pentru rezolvarea incidentelor cibernetice.
- Înțelegerea anatomiei atacurilor cibernetice din trecut este crucială pentru consolidarea apărării și încurajarea rezilienței în fața amenințărilor viitoare.

9.2. Exemple de bune practici

- Punerea în aplicare a NIS 2 marchează o nouă eră în reglementarea securității cibernetice în cadrul UE, una care necesită un nivel ridicat de vigilență și responsabilitate din partea companiilor;
- O strategie de răspuns la incidente cibernetice este vitală pentru orice organizație, având în vedere că trei sferturi dintre atacurile cibernetice care au reușit să pătrundă în sistemele de securitate ale organizațiilor au dus la pierderi financiare semnificative pentru companii;
- Dezvoltarea unei reziliențe puternice și munca continuă pentru a crește maturitatea în fața riscului cibernetic sunt esențiale pentru organizații. Asigurarea cibernetică ar trebui să completeze, nu să înlocuiască, o postură robustă de securitate cibernetică ;
- Organizațiile ar trebui:
  - Să se supună unor evaluări ale maturității securității cibernetice înainte de a aplica;
  - Acoperirea riscurilor cibernetice legate de lanțul de aprovizionare (întreruperi cauzate de furnizori);
  - Includerea clauzelor de întrerupere a activității și de amendă de reglementare;
  - Alinierea politicilor cu pragurile de incidente NIS2.

9.3. Amenințările comune includ:

- **Ransomware:** Atacatorii criptează datele unei organizații și solicită o răscumpărare pentru a restabili accesul. În 2021, ransomware-ul la nivel global a provocat daune de 18 miliarde de euro, de 57 de ori mai multe decât în 2015;
- **Malware: malware-ul,** cum ar fi virușii, viermii și troienii, poate afecta un sistem;

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.

- **Inginerie socială:** Înșelarea victimelor pentru a oferi acces neautorizat la sisteme sau servicii, cel mai adesea prin phishing. Aproape 60% din intrările în sistemul de securitate includ o componentă de inginerie socială;
- **Amenințări de date:** acces neautorizat și scurgeri de date, unde cea mai frecventă motivație este obținerea de bani;
- **Amenințări de disponibilitate:** atacuri care blochează accesul la date și servicii, cum ar fi atacurile DDoS;
- **Dezinformare:** Distribuirea de informații înșelătoare pentru a provoca frică și incertitudine;
- **Amenințări în lanțul de aprovizionare:** Atacuri asupra furnizorilor și clienților, care pot fi dificil de supravegheat din cauza sistemelor complexe și a multitudinii de furnizori;
- **Parole slabe:** parolele ușor de ghicit sau de spart sunt o vulnerabilitate majoră;
- **Utilizatori rău intenționați sau neinstruiți:** erorile utilizatorilor și angajații nemulțumiți pot compromite securitatea.

Sectoarele cel mai frecvent afectate de amenințările cibernetice sunt administrația publică, furnizorii de servicii digitale, publicul larg, sectorul serviciilor, sectorul financiar/bancar și sectorul sănătății.

SECȚIUNEA 10: RESURSE ȘI INSTRUMENTE UTILE

10.1. Instrumente și resurse utile pentru securitatea cibernetică

- **Liste de verificare a securității cibernetice:** Utilizarea listelor de verificare pentru implementarea măsurilor de securitate;
- **Ghiduri și standarde de referință:** Resurse recomandate pentru aprofundarea cunoștințelor;
- **Instrumente software recomandate:** Soluții de securitate cibernetică.

10.2. Alte recomandări

- Instalarea de software de securitate special conceput pentru dispozitive mobile, capabil să detecteze și să elimine viruși și să blocheze mesajele spam.
- Implementarea unei politici de securitate și aducerea acesteia în atenția tuturor angajaților.
- Utilizarea unui client VPN pentru a accesa rețeaua companiei de la distanță și implementarea autentificării 2FA/MFA.
- Implementarea măsurilor de securitate a e-mailului, cum ar fi SPF, DKIM și DMARC, activarea criptării mesajelor și utilizarea unei soluții de prevenire a pierderii datelor.
- Menținerea sistemelor de operare actualizate, instalarea unei soluții antivirus/antimalware și scanarea periodică a sistemului.
- Limitarea cantității de informații expuse public despre sistem sau organizație și implementarea controalelor de securitate, cum ar fi firewall-urile, criptarea și autentificarea.
- Copierea de rezervă a datelor și sistemelor critice și segmentarea rețelelor pentru a limita mișcarea atacatorilor.
- Efectuarea de audituri regulate de securitate pentru identificarea vulnerabilităților.

10.2.1. Exemplu

Ransomware Playbook (sintetic)

- ***Detectare:*** *alertă antivirus/EDR/SIEM;*
- ***Izolare:*** *deconectarea imediată a sistemului infectat;*
- ***Notificare:*** *incident manager, CSIRT, top management;*
- ***Evaluare:*** *ce sisteme sunt afectate? Backup-urile sunt intacte?*
- ***Notificare DNSC:*** *dacă există un incident major;*
- ***Corecție:*** *restaurare din backup, actualizări, schimbarea parolelor;*
- ***Raport final:*** *lecții învățate, revizuirea politicilor.*

🔐 *Toate etapele trebuie documentate și aprobate de conducere.*

Politica de securitate minimă (exemplu entitate BASIC)

Conținut recomandat:

- *scop și obiective;*
- *Aplicare;*
- *responsabilități (IT, management, utilizatori);*
- *controale de bază (MFA, backup, patching);*
- *politicieni de acces, cuvinte, criptare;*
- *plan de răspuns la incidente și revizuire anuală.*

Este revizuit anual sau după incidente majore. Aprobarea este obligatorie de către conducerea executivă.

CONCLUZIE

Cu amenințările cibernetice în creștere și reglementările din ce în ce mai stricte, organizațiile alimentare trebuie să trateze securitatea cibernetică ca pe o prioritate strategică, nu doar ca pe o obligație legală.

Acest ghid oferă nu doar o interpretare a cerințelor legale ale Directivei NIS2 și ale legislației naționale (OUG 155/2024, Legea 58/2023, Modificarea Legii privind securitatea cibernetică, nr. 51-402-01-17, prezentat de Consiliul de Miniștri Adunării Naționale la 12 decembrie 2024, adoptat la primul vot la 20 februarie 2025), ci și un set de măsuri practice și aplicabile care pot fi implementate treptat, în funcție de specificul fiecărei organizații.

Prin creșterea gradului de conștientizare, evaluarea riscurilor, implementarea măsurilor tehnice și organizaționale și construirea unei culturi a securității cibernetice, companiile alimentare pot:

- protejarea siguranței alimentare;
- prevenirea blocajelor în lanțul de aprovizionare;
- să respecte cerințele de conformitate;
- și menținerea încrederii clienților și partenerilor.

Invităm toate organizațiile să folosească acest ghid ca **punct de plecare pentru o transformare durabilă**, consolidându-și capacitățile digitale într-un mod responsabil, rezilient și adaptat provocărilor actuale.

"Securitatea cibernetică nu este doar un obiectiv IT – este o responsabilitate organizațională".

Versiunea oficială a Ghidului este în limba engleză, iar la nivel național, în România și Bulgaria, va fi publicat în limbile oficiale ale acestor țări, respectiv română și bulgară.

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.