NIS 2

2024

1 Introducere 3

1.1 Ce este NIS 2? 3

1.2 Pe cine afectează directiva NIS 2? 3

2 Cerințe NIS 2 4

2.1 Pentru entitățile esențiale și importante 4

3 Impactul asupra furnizorilor 4

4 Răspunsul companiei Axis 5

4.1 Securitate încă din momentul conceperii 5

4.2 Actualizări și corecții periodice 6

4.3 Autentificare și autorizare 6

4.4 Criptarea datelor 7

4.5 Raportarea incidentelor 7

4.6 Considerente legate de confidențialitate 8

4.7 Securitatea lanțului de aprovizionare 8

4.8 Instruire și îndrumare 9

1 Introducere

1.1 Ce este NIS 2?

NIS 2 este o directivă UE care trebuie transpusă în legislația națională a fiecărui stat membru al UE până la data de 17 octombrie 2024. NIS 2 are ca scop atingerea aceluiași nivel înalt de securitate cibernetică pe întregul teritoriu al Uniunii Europene, pentru a contribui la securitatea regiunii și funcționarea eficientă a economiei și societății acesteia. Directiva impune ca entitățile care furnizează servicii esențiale și importante în sectoarele cheie ale societății să dezvolte capabilități de securitate cibernetică, să diminueze amenințările la adresa rețelei și sistemelor informatice, să asigure continuitatea serviciilor în cazul producerii oricăror incidente și să raporteze incidentele de securitate autorităților relevante. De asemenea, le impune statelor membre să adopte strategii de securitate cibernetică la nivel național și să înființeze anumite autorități, inclusiv autorități de gestionare a situațiilor de criză cibernetică și echipe de intervenție în cazul producerii oricăror incidente de securitate informatică. Directiva prezintă măsurile de gestionare a riscurilor la adresa securității cibernetice, precum și măsurile de implementare care trebuie luate. Nerespectarea directivei de către entitățile esențiale și importante poate atrage după sine amenzi mari și poate avea ramificații legale pentru echipele de management.

Pentru mai multe informații, vizitați:
eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1713340785613

1.2 Pe cine afectează directiva NIS 2?

Directiva NIS 2 afectează toate entitățile care furnizează servicii **esențiale** sau **importante** economiei și societății europene, inclusiv societățile comerciale și furnizorii.

1.2.1 Persoane și entități afectate direct

Entități esențiale – Entități din următoarele domenii: energie, transport, bănci/finanțe, sănătate, apă potabilă, apă reziduală, infrastructură digitală, administrație publică, spațiu

Entități importante – Entități din următoarele domenii: servicii poștale, gestionarea deșeurilor, produse chimice, alimentație, fabricație (de exemplu, dispozitive medicale, echipamente electrice, echipamente de transport); furnizori digitali (de exemplu, piețe online, motoare de căutare, rețele de socializare), organizații de cercetare

Autorități naționale competente – Autoritățile naționale competente sunt desemnate de statele membre ale UE pentru a monitoriza modul în care este implementată și pusă în aplicare directiva NIS 2 în țările respective.

1.2.2 Persoane și entități afectate indirect

Furnizorii și distribuitorii – Directiva NIS 2 afectează indirect distribuitorii, furnizorii și prestatorii de servicii terți care furnizează servicii esențiale sau servicii digitale entităților esențiale și importante. Aceste companii trebuie să asigure securitatea produselor și serviciilor pe care le oferă și pot fi obligate să respecte anumite cerințe contractuale referitoare la securitatea cibernetică impuse de clienți.

Utilizatorii de servicii esențiale și servicii digitale – Deși nu se află direct sub incidența directivei NIS 2, utilizatorii de servicii esențiale și servicii digitale beneficiază de pe urma practicilor de securitate cibernetică îmbunătățite și a capabilităților de reacție în caz de incidente impuse de aceasta. Acest lucru sporește indirect securitatea și fiabilitatea serviciilor pe care se bazează.

2 Cerințe NIS 2

2.1 Pentru entitățile esențiale și importante

Măsuri de securitate – Să implementeze măsuri de securitate adecvate pentru gestionarea riscurilor și garantarea securității rețelei și sistemelor informatice proprii. Aceste măsuri trebuie să se bazeze pe evaluări ale riscurilor și cele mai bune practici.

Raportarea incidentelor – Să raporteze autorităților competente toate incidentele semnificative care ar putea avea un impact important asupra securității rețelei și sistemelor informaționale proprii. Raportarea în timp util este esențială pentru coordonarea intervențiilor și reducerea potențialelor efecte negative.

Gestionarea riscurilor – Să efectueze evaluări ale riscurilor în vederea identificării posibilelor amenințări și vulnerabilități, și să adopte măsuri pentru diminuarea acestor riscuri.

Cooperarea cu autoritățile competente – Să coopereze cu autoritățile competente desemnate de statele membre ale UE. Aceasta include furnizarea informațiilor necesare și permiterea accesului la sisteme în scopul supravegherii reglementare și al facilitării răspunsului la incidentele produse.

Planificarea răspunsului la incidente – Să dezvolte și să mențină planuri de răspuns la incidente, pentru a putea interveni în mod eficient în cazul producerii oricăror incidente de securitate cibernetică. Aceste planuri trebuie să prezinte procedurile care trebuie efectuate pentru detectarea și raportarea incidentelor, precum și pentru diminuarea consecințelor acestora.

Securitatea lanțurilor de aprovizionare – Să securizeze lanțurile de aprovizionare, inclusiv la nivelul furnizorilor și distribuitorilor terți, pentru a asigura reziliența generală a rețelei și a sistemelor informatice.

Monitorizare continuă – Să implementeze o monitorizare și auditare continuă a rețelei și a sistemelor informatice pentru a putea detecta și răspunde la amenințări și vulnerabilități în timp real.

3 Impactul asupra furnizorilor

Furnizorii pot susține entitățile NIS 2 prin respectarea următoarelor cerințe:

Securitate încă din momentul conceperii – Producătorii de dispozitive IoT trebuie să încorporeze funcții de securitate în dispozitivele lor încă din faza de proiectare, asigurându-se astfel că securitatea este o parte integrantă a produsului.

Actualizări și corecții periodice – Producătorii trebuie să ofere periodic corecții și actualizări de securitate pentru a rezolva orice vulnerabilități prezente în dispozitivele IoT pe care le oferă.

Autentificare și autorizare – Dispozitivele IoT trebuie să dispună de mecanisme de autentificare puternice și controale adecvate ale permisiunilor, pentru a preveni accesul neautorizat.

Criptarea datelor – Transmiterea și stocarea datelor de către dispozitivele IoT trebuie criptate pentru a preveni interceptarea sau accesarea informațiilor sensibile de către persoane neautorizate.

Raportarea incidentelor – Producătorii trebuie să raporteze autorităților relevante și, posibil, consumatorilor sau clienților, toate incidentele sau breșele de securitate semnificative apărute în legătură cu dispozitivele lor IoT.

Considerente legate de confidențialitate – Dispozitivele IoT care prelucrează date cu caracter personal trebuie să respecte nu numai Directiva NIS 2 privind securitatea cibernetică, ci și reglementările privind protecția datelor, precum Regulamentul general privind protecția datelor (RGPD).

Securitatea lanțului de aprovizionare – Garantarea securității întregului lanț de aprovizionare, de la furnizorii componentelor până la clienți, este obligatorie pentru a preveni introducerea în procesul de producție, în orice moment, a vulnerabilităților de securitate.

4 Răspunsul companiei Axis

Mai jos este prezentat modul în care Axis, în calitate de furnizor, întrunește cerințele aplicabile entităților NIS 2:

4.1 Securitate încă din momentul conceperii

Axis a adoptat o abordare axată pe securitatea implicită, încă din momentul conceperii, pentru a garanta faptul că activitățile și considerentele de securitate formează o parte integrală a procesului de proiectare și dezvoltare a produselor, în vederea reducerii riscului de apariție a vulnerabilităților și a integrării implicite în cadrul produselor a unor configurații de securitate robuste. În cadrul companiei Axis, principiul securității implicite, încă din momentul conceperii, se aplică atât produselor software, cât și echipamentelor hardware, conținând următoarele patru elemente principale:

- *Modelul de dezvoltare a produselor de securitate Axis (Axis Security Development Model, ASDM)*: ASDM este un cadru de procese definite și instrumente care garantează integrarea considerentelor de securitate în procesul de dezvoltare software. Activitățile includ efectuarea de evaluări ale riscului, modelarea amenințărilor, testarea penetrabilității, scanarea pentru depistarea vulnerabilităților, gestionarea incidentelor și programul de recompensare pentru identificarea erorilor. Dezvoltatorii programelor software Axis utilizează modelul ASDM pentru a se asigura că securitatea este integrată în procesul de dezvoltare software, în vederea reducerii riscului de lansare a unor produse software care conțin vulnerabilități.

- *Programul de recompensare pentru identificarea erorilor*: Axis susține un program privat de recompensare pentru identificarea erorilor care sprijină eforturile companiei de a identifica, corecta și dezvălui în mod proactiv vulnerabilitățile din AXIS OS, sistemul de operare pe bază de Linux care se regăsește pe majoritatea produselor Axis. Acest program întărește angajamentul companiei Axis de a clădi relații profesionale solide cu cercetătorii din domeniul securității și hackerii etici din afara organizației sale.

- *Lista de materiale software (SBOM)*: Axis furnizează o listă SBOM pentru AXIS OS, sistemul de operare bazat pe Linux care este utilizat pe majoritatea dispozitivelor Axis. Aceasta le oferă cercetătorilor din domeniul securității, autorităților și clienților informații despre componentele software care alcătuiesc sistemul AXIS OS. Lista este utilă în special entităților specializate în evaluarea vulnerabilităților și analiza riscurilor, făcând dovada angajamentului companiei Axis de a promova transparența în securitatea cibernetică.

- *Setările de securitate implicite ale sistemului AXIS OS*: Dispozitivele echipate cu cele mai noi versiuni AXIS OS sunt preconfigurate din fabrică după cum urmează: fără parolă implicită; compatibilitate cu HTTP și HTTPS; integrare și comunicații securizate, cu standardul IEEE 802.1X/802.1AR/802.1AE activat în mod implicit; dezactivarea protocoalelor mai puțin sigure. Mai multe informații despre controalele de protecție implicite pot fi accesate *aici*.

- *Axis Edge Vault*: Axis Edge Vault este o platformă de securitate pe bază de hardware integrată în produsele Axis, care include funcții ce protejează integritatea produselor de rețea Axis și permite executarea de operațiuni securizate pe bază de chei criptografice. Pentru a proteja lanțul de aprovizionare, platforma oferă o funcție de boot securizat și OS semnat; identitate de încredere a dispozitivelor, conferită de identificatorul unic încorporat al dispozitivelor Axis, pentru dovedirea originii

dispozitivului; stocare securizată a cheilor, pentru păstrarea în siguranță a informațiilor criptografice; și utilizarea unei funcții de video semnat pentru detectarea interferării cu înregistrările video.

4.2 Actualizări și corecții periodice

Axis furnizează actualizări de software pentru a rezolva, printre altele, vulnerabilitățile de securitate nou descoperite la nivelul produselor sale hardware și software. De asemenea, Axis pune la dispoziție instrumentele de gestionare a dispozitivelor care le permit clienților să actualizeze mai ușor și cu regularitate software-ul dispozitivelor Axis pe care le dețin. Noile versiuni AXIS OS destinate dispozitivelor conectate sunt evidențiate în AXIS Companion, AXIS Camera Station și sistemele de video management ale partenerilor, cum ar fi Milestone XProtect® și Centrul de securitate Genetec™, precum și în instrumentele de gestionare a dispozitivelor Axis. În plus, Axis oferă un serviciu de notificare în materie de securitate, la care se poate abona oricine. Informații mai detaliate sunt prezentate mai jos.

- *AXIS OS*: Axis oferă două alternative principale pentru actualizarea software-ului dispozitivelor: pista activă și pista de suport pe termen lung (LTS). Pista activă oferă acces la cele mai noi funcții și funcționalități de ultimă generație, precum și la remedieri ale erorilor și corecții de securitate. Programele software incluse în pistele de suport pe termen lung (LTS) maximizează stabilitatea furnizând doar remedieri ale erorilor și corecții de securitate, deoarece accentul se pune pe menținerea unui sistem terț bine integrat.
- Instrumentele de gestionare a dispozitivelor: *AXIS Device Manager* și *AXIS Device Manager Extend* sunt instrumente care ajută clienții să își actualizeze în mod regulat programele software de pe dispozitivele Axis deținute cu cele mai recente corecții de securitate și remedieri ale erorilor.

  Pentru configurarea și gestionarea eficientă a dispozitivelor Axis la nivel local, AXIS Device Manager permite procesarea pe loturi a sarcinilor de securitate, precum gestionarea acreditărilor dispozitivelor, implementarea certificatelor, dezactivarea serviciilor care nu sunt utilizate și actualizarea sistemului AXIS OS.

  AXIS Device Manager Extend oferă o interfață agregată care reunește informații despre toate dispozitivele și locațiile dumneavoastră într-o singură aplicație ușor de utilizat. Aplicația vă notifică atunci când sunt disponibile actualizări software pentru dispozitive și vă permite să efectuați actualizări în masă și alte sarcini la scară largă. În plus, veți primi recomandări referitoare la produsele de schimb. Toate activitățile sunt pe deplin trasabile, fiind posibilă exportarea tuturor informațiilor aferente dispozitivelor din sistem în scopuri de raportare sau auditare.
- *Serviciul Axis de notificare în materie de securitate*: Acest serviciu, la care Axis încurajează pe toată lumea să se aboneze, le trimite abonaților notificări în timp util cu privire la incidentele și vulnerabilitățile de securitate.

4.3 Autentificare și autorizare

Pentru a preveni accesul neautorizat și a spori securitatea generală a dispozitivelor sale, Axis suportă:

- Drepturile de acces pe bază de roluri în vederea gestionării dispozitivelor (Administrator/Operator/Vizualizator) și posibilitatea de a centraliza procesul de autentificare/autorizare prin conectarea dispozitivelor Axis la soluții IT integrate și standardizate care utilizează tehnologia *Active Directory Federation Service* (ADFS) . (ADFS este o componentă software dezvoltată de Microsoft pentru a oferi un serviciu de autorizare prin conectare unică (Single Sign-On, SSO) persoanelor care utilizează sisteme de operare de tip Windows Server. ADFS le permite utilizatorilor

din diferite organizații să acceseze aplicații aflate pe sistemele de operare de tip Windows Server folosind un singur set de acreditări de conectare).

- Tehnologii care ușurează *interconectarea cu nivel de încredere zero* . În cele mai recente versiuni AXIS OS, aceste tehnologii includ identificatoare ale dispozitivelor Axis care respectă standardele IEEE 802.1X și IEEE 802.1AR, pentru instalarea automată și securizată a dispozitivelor într-o rețea cu certificare IEEE 802.1X, precum și standardul IEEE 802.1AE (MACsec) pentru criptarea automată a comunicațiilor de date.

4.4 Criptarea datelor

Pentru a proteja informațiile sensibile împotriva interceptării sau accesării de persoane neautorizate, produsele Axis acceptă:

- Protocolul HTTPS, unde toate comunicațiile de date respectă protocolul TLS 1.2 sau standarde mai noi. Conexiunea de flux video dintre serverul sistemului de video management AXIS Camera Station și client este criptată conform standardului AES-256.
- Standardul *IEEE 802.1AE (MACsec)* pentru criptarea automată a comunicațiilor de date.
- Transmisii video securizate prin protocolul RTP, denumit și SRTP/RTSPS (începând cu versiunea AXIS OS 7.40). Protocolul SRTP/RTSPS utilizează o metodă de transport criptat securizat complet, pentru a se asigura că fluxul video transmis de dispozitivul Axis este recepționat numai de clienții autorizați în acest sens.
- *Criptarea stocării la marginea rețelei* (card SD)
- *Exportarea criptată cu parolă a înregistrărilor realizate la marginea rețelei* (card SD, partajare prin rețea), începând cu versiunea AXIS OS 10.10. Aceasta face posibilă exportarea unei înregistrări care este protejată prin parolă, adăugând posibilitatea de a partaja în siguranță datele video sensibile fără a mai fi necesară criptarea manuală a înregistrărilor exportate.

4.5 Raportarea incidentelor

Axis oferă o funcție de raportare a incidentelor sau vulnerabilităților de securitate descoperite în produsele și serviciile sale.

- Axis deține rolul de autoritate de numerotare în cadrul Programului de vulnerabilități și expuneri comune (CVE). Aceasta înseamnă că Axis implementează cele mai bune practici din industria de profil pentru a gestiona și a răspunde - cu transparență - la vulnerabilitățile descoperite la nivelul produselor și serviciilor sale, pentru a minimiza riscul de expunere al clienților. De asemenea, Axis poate aloca numere CVE vulnerabilităților nou descoperite, pe care le va raporta pe site-ul web *www.cve.org*. *Politica de gestionare a vulnerabilităților* a companiei Axis este publicată pe site-ul web axis.com.
- Oricine se poate abona *aici* pentru a primi o notificare de securitate din partea companiei Axis.
- Noile versiuni AXIS OS includ corecții de securitate și remedieri ale erorilor. Disponibilitatea software-ului actualizat al dispozitivelor este, de asemenea, evidențiată în AXIS Companion, AXIS Camera Station, AXIS Device Manager, AXIS Device Manager Extend și unele sisteme VMS terțe, precum Milestone XProtect și Centrul de securitate Genetec.
- Axis promovează transparența în legătură cu orice atacuri cibernetice legate de organizația sa și va raporta aceste incidente în conformitate cu îndrumările furnizate de autoritățile suedeze relevante.

4.6 Considerente legate de confidențialitate

Compania Axis își publică *politica de confidențialitate* și notificarea privind confidențialitatea pe platforma sa online, unde explică detaliat ce date cu caracter personal sunt colectate (de exemplu, dintr-un cont My Axis online) și cum sunt utilizate acestea.

De asemenea, Axis și-a publicat *cadrul și practicile de securitate cibernetică* legate de Sistemul său de gestionare a securității informațiilor, care dispune de certificare ISO/IEC 27001. Domeniul de aplicare al certificatului ISO/IEC 27001 deținut de Axis acoperă dezvoltarea și exploatarea infrastructurii și serviciilor informatice interne. ISO 27001 este un standard recunoscut pe plan internațional care oferă îndrumări cu privire la protejarea și gestionarea informațiilor unei organizații printr-un management eficient al riscurilor.

Conformitatea cu standardul *ISO/IEC 27001* demonstrează că Axis utilizează cele mai bune practici și procese recunoscute pe plan internațional pentru a își gestiona infrastructura și sistemele informaționale interne care sprijină și furnizează servicii clienților și partenerilor.

De asemenea, Axis își ajută clienții să răspundă preocupărilor legate de confidențialitate în domeniul supravegherii în ceea ce privește realizarea înregistrărilor video și audio. Soluțiile includ:

- Mascarea statică a zonelor de confidențialitate pe camerele Axis și mascarea dinamică a zonelor de confidențialitate cu ajutorul aplicației software *AXIS Live Privacy Shield*
- Sisteme de analiză la marginea rețelei, precum aplicația *AXIS People Counter* sau *AXIS P8815-2 3D People Counter*, care captează și stochează numai date numerice statistice — nu sunt prelucrate niciun fel de informații de identificare personală
- *Camere termice*
- *Produse radar*
- Instrumentul de cenzurare video din aplicația *AXIS Camera Station* pentru mascarea obiectelor sau a zonelor care nu prezintă interes
- *Capabilitățile audio dezactivate în mod implicit* în produsele de supraveghere video oferite de Axis

Mai multe informații referitoare la soluțiile de protejare a confidențialității sunt disponibile la *axis.com/solutions/privacy-in-surveillance*

4.7 Securitatea lanțului de aprovizionare

Securizarea întregului lanț de aprovizionare, de la furnizorii de componente până la clienți, este importantă în prevenirea introducerii oricăror vulnerabilități de securitate.

În abordarea securității cibernetice, Axis se axează pe *ciclul de viață al produselor*. Suntem hotărâți să reducem la minimum riscurile, nu doar în cadrul întregului lanț de aprovizionare, de la nivel de componentă până la produsul finit, ci și în timpul distribuției și implementării, precum și în fazele de exploatare și de scoatere din funcțiune.

Următoarele sunt doar câteva dintre modalitățile în care Axis abordează securitatea lanțului de aprovizionare:

- Axis achiziționează componentele critice direct de la furnizori strategici. Colaborăm îndeaproape cu partenerii noștri de fabricație. Procesele de producție sunt monitorizate, iar datele sunt partajate non-stop cu Axis, permițând analizarea acestora în timp real și facilitând transparența. Aflați mai multe despre *securitatea lanțului de aprovizionare al companiei Axis*.

- Securitate integrată a dispozitivelor prin intermediul aplicației Axis Edge Vault, care protejează integritatea dispozitivelor Axis cu ajutorul următoarelor funcții:
  - **Sistem de operare (OS) semnat**: Garantează faptul că sistemul AXIS OS este furnizat de Axis. În plus, se asigură că orice versiune AXIS OS nouă care urmează a fi instalată pe dispozitiv este, de asemenea, semnată de Axis.
  - **Boot securizat**: Permite dispozitivului să verifice dacă sistemul de operare prezintă semnătura Axis. Dacă sistemul de operare este neautorizat sau a fost modificat, procesul de inițializare este abandonat și dispozitivul se oprește din funcționare. Sistemul de operare (OS) semnat este combinat cu funcția de boot securizat și efectuarea unei resetări din fabrică, pentru a oferi protecție împotriva tentativelor de modificare în timpul transportului dispozitivului.
  - **Identificatorul dispozitivului Axis** respectă standardul IEEE 802.1AR, ceea ce permite identificarea securizată a dispozitivului și instalarea în siguranță a acestuia într-o rețea. Identificatorul dispozitivului Axis este stocat în depozitul de chei securizat al dispozitivului (element securizat, TPM, TEE).
  - **Sistemul de fișiere criptate** protejează configurația și informațiile specifice clientului stocate în sistemul de fișiere împotriva extragerii sau manipulării neautorizate atunci când dispozitivul nu este în funcțiune, de exemplu în timpul transportului de la integratorul de sistem la client.
  - În plus, suportul pentru **video semnat** oferit de Axis le permite vizualizatorilor să verifice dacă înregistrările video au fost sau nu modificate în timpul exportării de pe un dispozitiv. Acest lucru este deosebit de important, în special în cadrul unei investigații sau urmăriri penale. Mai multe informații se găsesc la *axis.com/solutions/edge-vault*.
- Pe site-ul web axis.com se găsește o sumă de verificare pentru descărcările de software. Această sumă de verificare permite confirmarea integrității unui fișier.
- Certificare ETSI: Mai mult de 150 de produse Axis echipate cu sistem de operare AXIS OS 11 sau o versiune ulterioară a acestuia sunt certificate conform *standardului de securitate ETSI EN 303 645*. ETSI este acronimul pentru Institutul European de Standardizare în Telecomunicații. Cerințele acestuia se referă la dispozitivele în sine, inclusiv la suportul pentru funcțiile de securitate bazate pe hardware cum ar fi stocarea securizată a cheilor de criptare, precum și pentru funcțiile de securitate implicite cum ar fi activarea implicită a standardul HTTPS și neutilizarea parolelor implicite. Un alt aspect îl constituie gestionarea ciclului de viață, care implică definirea unei perioade de suport pentru efectuarea actualizărilor de securitate la nivelul dispozitivelor. Altele includ adoptarea unei metodologii pentru reducerea riscului de apariție a vulnerabilităților în procesul de dezvoltare a programelor software, implementarea unei politici de gestionare a vulnerabilităților și adoptarea celor mai bune practici în prelucrarea datelor cu caracter personal. Aceste cerințe iau în considerare cele mai bune practici din domeniu care garantează că produsele certificate dispun de un nivel minim de securitate de bază pe toată durata ciclului lor de viață. Standardul se aliniază îndeaproape cu legea UE privind reziliența cibernetică, directiva UE privind echipamentele radio și alte standarde și legi din întreaga lume.

4.8 Instruire și îndrumare

Axis oferă personalului propriu, partenerilor și clienților informații și instruire cu privire la cele mai bune practici în domeniul securității cibernetice. Acestea includ următoarele:

- Conștientizare și instruire la nivel intern cu privire la securitate: Axis a dezvoltat un program de conștientizare în materie de securitate pentru a se asigura că angajații săi sunt instruiți permanent pentru a putea evita și reduce amenințările la adresa securității organizației. Această instruire de conștientizare este obligatorie pentru toți membrii personalului Axis. În funcție de rolul și

responsabilitățile fiecăruia în cadrul organizației, dezvoltatorii și proprietarii de sisteme pot beneficia de instruire suplimentară în domeniul securității.

- *Instruire în cadrul Academiei Axis*: Clienților li se pun la dispoziție cursuri de instruire, care includ un curs online pe tematica securității cibernetice și *abordarea companiei Axis în ceea ce privește acest subiect*.
- *Ghiduri de îmbunătățire a securității* disponibile online pentru:
  - *AXIS OS*
  - *AXIS Camera Station*
  - *Comutatoarele de rețea Axis*
- *Ghidul privind utilizarea scanerului de securitate al AXIS OS*: Axis recomandă scanarea de securitate a dispozitivelor Axis, pentru a verifica dacă acestea sunt afectate de vulnerabilități sau o configurare deficitară. Ghidul privind utilizarea scanerului de securitate al AXIS OS oferă recomandări cu privire la modul în care pot fi remediate anumite rezultate ale scanării și prezintă rezultatele „fals pozitive" care sunt obținute frecvent.
- *Ghidul criminalistic AXIS OS*: Acest ghid oferă sfaturi tehnice pentru persoanele care efectuează analize criminalistice asupra dispozitivelor Axis în cazul unui atac la adresa securității cibernetice a rețelei înconjurătoare și infrastructurii informatice în care este instalat dispozitivul Axis.

Pentru mai multe informații despre Axis și securitatea cibernetică, vă rugăm să accesați *portalul Axis pentru securitate cibernetică*.

T10210486/RO/M3.3/24