DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Securitatea lanțului de aprovizionare software pentru IMM-uri

DECEMBRIE 2025

TLP:CLEAR

Cuprins

Introducere

Lanțul de aprovizionare software (LAS) reprezintă întregul circuit parcurs de un produs software de la faza de concepție până la livrarea către utilizatorul final. Securitatea LAS a devenit o preocupare majoră în ultimii ani, deoarece atacatorii cibernetici își modifică tacticile, vizând tot mai des furnizorii și partenerii companiilor. Protecția cibernetică la nivel intern nu mai este suficientă, întrucât atacatorii și-au mutat atenția către elementele din lanțul de aprovizionare[1]. Acest lucru este relevant în special pentru întreprinderile mici și mijlocii (IMM-uri), care adesea dispun de resurse limitate de securitate. Ele se bazează pe soluții software terțe sau pe serviciile unor furnizori externi. Conform evaluărilor specialiștilor[2], peste 78% dintre IMM-urile din România nu dispun de personal cu competențe în securitate cibernetică și nu implementează politici interne de protecție a sistemelor informatice. Lipsa unei infrastructuri IT bine gestionate le expune atât atacurilor directe, cât și celor care se propagă prin LAS.

Atacurile asupra LAS pot avea consecințe severe, depășind cu mult limitele organizației țintă inițiale. Într-un singur incident de anvergură, sute sau mii de companii pot fi afectate simultan prin compromiterea unui produs software folosit la scară largă. Acest aspect evidențiază necesitatea ca organizațiile, indiferent de dimensiune, să verifice software-ul și componentele terțe înainte de utilizare, pentru a se asigura că nu au fost compromise. În același timp, astfel de atacuri devin tot mai răspândite, deoarece compromiterea unui singur element din lanțul de aprovizionare poate afecta un număr extins de utilizatori și organizații.

Acest ghid își propune să ofere IMM-urilor informații practice despre LAS, riscurile actuale, cerințe legale și măsuri pentru a spori reziliența cibernetică. De asemenea, sunt prezentate exemple reale de incidente, lecțiile învățate din acestea, precum și o serie de instrumente gratuite sau accesibile care pot ajuta IMM-urile în gestionarea riscurilor asociate LAS.

Riscuri și amenințări

LAS include etapele de proiectare, dezvoltare, producție, integrare, implementare, configurare, utilizare și, eventual, retragerea din uz[3].

LAS este compus din actori, componente tehnice și infrastructura de distribuție[4] (Figura 1). Printre actorii implicați se numără echipele interne de dezvoltare, furnizorii de servicii IT, dezvoltatorii externi, integratorii și distribuitorii. Componentele tehnice includ codul sursă propriu, bibliotecile și componentele din surse deschise sau comerciale, precum și sistemele de integrare continuă și de generare a codului executabil. Ultima componentă din LAS este infrastructura de distribuție, reprezentată de servere de actualizare sau magazine de aplicații.

Fiecare verigă din acest lanț poate deveni o țintă pentru atacatori, motiv pentru care se afirmă că „securitatea unui lanț de aprovizionare este la fel de robustă ca cea mai slabă verigă a sa”.

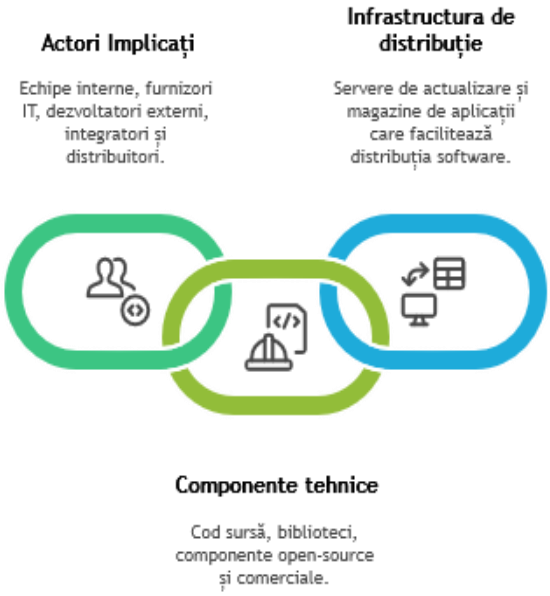

Figura 1. Lanțul de aprovizionare software

[1] https://digital-strategy.ec.europa.eu/ro/news/enisa-published-its-threat-landscape-supply-chain-attacks
[2] https://adrvest.ro/start-la-inscrieri-pentru-cybertm-2025-eveniment-privind-securitatea-cibernetica-dedicat-imm-urilor-din-regiunea-vest/
[3] https://securitatea-cibernetica.ro/documente/Legea-privind-securitatea-si-apararea-cibernetica-a-Romaniei.pdf
[4] CISA, 2021, Defending Against Software Supply Chain Attacks
https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508.pdf

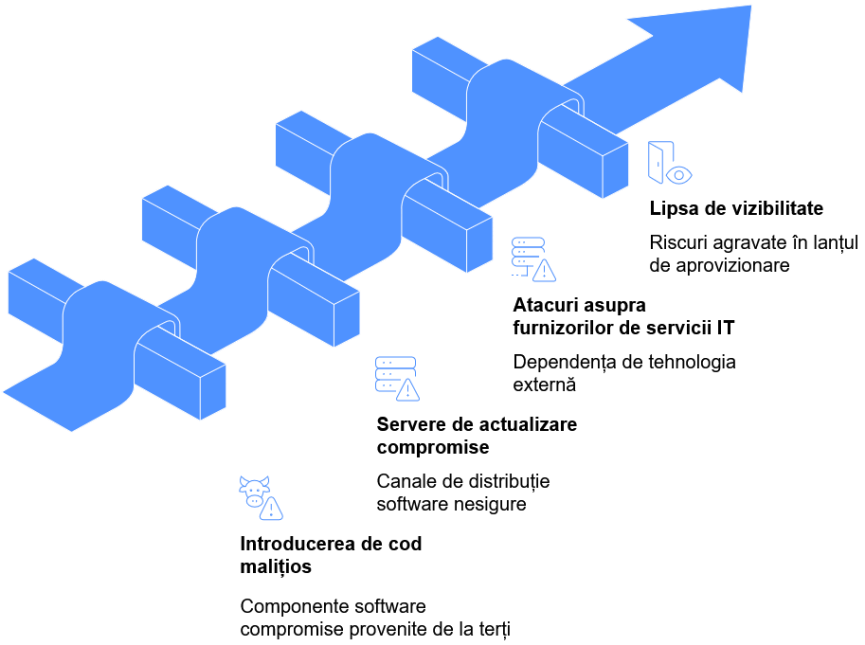

Figura 2. Riscuri asociate

Atacurile asupra LAS pot îmbrăca diferite forme. Ele se bazează pe exploatarea încrederii pe care organizațiile o acordă furnizorilor de produse și servicii.

Un risc major îl constituie **introducerea de cod malițios în componente software provenite de la terți**. Astfel de situații apar, de exemplu, atunci când o bibliotecă din surse deschise sau un pachet dintr-un registru public este compromis. În momentul în care o organizație își actualizează aplicația cu acel pachet, importă fără să știe și un program malițios.

Au fost documentate cazuri în care atacatorii au publicat numeroase pachete false, cu denumiri asemănătoare celor legitime. Această tehnică, numită typosquatting, urmărește infectarea stațiilor de lucru ale dezvoltatorilor și furtul de date sensibile[5] (a se vedea anexele).

O altă categorie de risc o constituie compromiterea **serverelor de actualizare sau a canalelor de distribuție** ale unui furnizor de software.

Atacurile asupra furnizorilor de servicii IT amenință IMM-urile[6], care depind de furnizorii externi de tehnologie. Un atac asupra furnizorului se transmite automat către clienți, care devin victime colaterale, deși nu erau ținta inițială. Nu în ultimul rând, **lipsa vizibilității și a transparenței** pe lanțul de aprovizionare agravează riscurile.

În două treimi dintre incidentele de pe LAS analizate de ENISA[7], furnizorii nu au cunoscut sau nu au raportat modalitatea prin care a avut loc atacul. În schimb, 91% dintre clienții afectați au declarat că au fost informați despre vectorul de atac, ceea ce arată o transparență ridicată la nivelul organizațiilor care au fost afectate. Acest decalaj informativ reflectă dificultatea furnizorilor de a detecta rapid breșele și de a transmite alertele necesare către părțile afectate.

Pentru IMM-uri, un atac nedetectat poate însemna o expunere prelungită la acces neautorizat și compromiterea continuă a datelor. Pe lângă efectele tehnice, astfel de situații pot afecta încrederea utilizatorilor și pot genera consecințe juridice, inclusiv în raport cu obligațiile contractuale și normele de protecție a datelor.

---

[5] https://thehackernews.com/2023/02/python-developers-beware-clipper.htm
[6] https://www.reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05/
[7] ENISA, 2023, Good Practices for Supply Chain Cybersecurity, https://www.enisa.europa.eu/sites/default/files/publications/Good%20Practices%20for%20Supply%20Chain%20Cybersecurity.pdf

Amenințări emergente în LAS

Pe lângă vectorii clasici (inserarea de cod malițios, compromiterea serverelor de actualizare sau atacurile asupra furnizorilor de servicii IT), în ultimii ani s-au conturat noi forme de amenințări:

1. **Compromiterea intenționată a contribuțiilor open-source:** cazul **XZ Utils (2024)** a arătat că atacatorii pot pătrunde treptat în proiecte cu **cod sursă deschis**, devenind colaboratori aparent de încredere și introducând ulterior cod malițios direct în componentele software legitime. Astfel de atacuri sunt dificil de depistat, deoarece exploatează **încrederea comunității de dezvoltatori** și lipsa unui control centralizat al modificărilor;

2. **Exploatarea lanțului de integrare continuă (CI/CD)**: mediile automatizate de compilare și testare pot fi compromise, permițând modificarea pachetelor software chiar înainte de distribuire. Accesul neautorizat la aceste sisteme oferă atacatorilor posibilitatea de a insera cod malițios semnat digital, așa cum s-a observat în incidentele SolarWinds și 3CX (2023);

3. **Dependențele indirecte și scripturile de instalare**: componentele software care par sigure pot depinde la rândul lor, de alte biblioteci vulnerabile sau compromise. Atacurile care vizează aceste legături dintre dependențe, inclusiv prin scripturi executate automat la instalare, sunt tot mai frecvente și dificil de prevenit fără o evidență și o verificare atentă a tuturor pachetelor utilizate.

În plus, creșterea utilizării instrumentelor de inteligență artificială (IA) în dezvoltarea software introduce riscuri suplimentare, precum includerea automată a fragmentelor de cod neverificate din surse publice.

În concluzie, LAS introduce un **profil de risc complex** pentru IMM-uri. Orice componentă software externă sau serviciu tehnologic contractat poate deveni poarta de intrare a unui atac cibernetic, dacă nu sunt implementate măsuri adecvate de verificare și securizare. Reputația și continuitatea afacerii pot fi grav afectate de un incident apărut „din amonte", în afara perimetrului tradițional al organizației. Pentru a face față acestor provocări, IMM-urile trebuie să adopte o abordare sistematică de gestionare a riscurilor pe lanțul de aprovizionare.

Cadrul european și reglementări relevante

Securitatea lanțului de aprovizionare software a devenit o prioritate în cadrul legislativ european, odată cu adoptarea unor standarde mai stricte de protecție cibernetică aplicabile întregii economii. Pe lângă Directiva NIS2[8] și Regulamentul privind Reziliența Cibernetică (Cyber Resilience Act – CRA)[9], alte inițiative precum Digital Operational Resilience Act (DORA)[10], Cybersecurity Act[11] și Cyber Solidarity Act[12], consolidează cadrul unitar de reziliență cibernetică al UE. Toate aceste reglementări sunt aplicabile și în România, contribuind la alinierea legislației naționale la cerințele europene.

Directiva NIS2 (UE 2022/2555)

Adoptată la finalul anului 2022, Directiva NIS2 înlocuiește vechea directivă NIS (2016) și stabilește un cadru comun de securitate a rețelelor și sistemelor informatice în toate statele membre. Directiva extinde aria de aplicare și impune cerințe mai stricte pentru entitățile considerate esențiale și importante. Un element central este includerea explicită a riscurilor din lanțul de aprovizionare în politicile de securitate. Conform articolului 21, organizațiile vizate trebuie să implementeze măsuri tehnice și organizaționale adecvate pentru gestionarea acestor riscuri. În România directiva NIS2 a fost transpusă în legislația internă prin Legea 124/2025[13] (care a aprobat OUG 155/2024) și a fost operaționalizată prin două ordine ale Directoratului Național de Securitate Cibernetică (DNSC) care au intrat în vigoare în august 2025[14].

În Romania, Directiva NIS2 se aplică tuturor organizațiilor mijlocii și mari din sectoare precum energie, transporturi, sănătate, infrastructuri digitale, servicii financiare sau administrație publică centrală. IMM-

[8] https://digital-strategy.ec.europa.eu/ro/policies/nis2-directive
[9] https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=OJ:L_202402847#art_3
[10] https://eur-lex.europa.eu/RO/legal-content/summary/digital-operational-resilience-for-the-financial-sector.html
[11] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=legissum%3A4398780
[12] https://eur-lex.europa.eu/eli/reg/2025/38/oj
[13] https://legislatie.just.ro/public/DetaliiDocument/299675
[14] https://www.dnsc.ro/pagini/legislatie-nis2

urile sunt în general exceptate, însă cele care furnizează servicii critice sau se încadrează în categoriile de entități esențiale ori importante pot intra sub incidența directivei. Directiva promovează ideea de responsabilitate extinsă: organizațiile vor solicita furnizorilor să respecte standarde minime de securitate, pentru a proteja LAS.

Din perspectiva conformării, directiva introduce cerințe concrete privind managementul riscurilor, raportarea incidentelor și documentarea măsurilor adoptate. Entitățile trebuie să notifice incidentele majore în termen de 24 de ore (alertă inițială) și 72 de ore (raport complet). Directiva aplică principiul proporționalității, astfel măsurile de securitate trebuie adaptate dimensiunii și nivelului de risc al organizației. Nerespectarea prevederilor poate atrage sancțiuni de până la 10 milioane de euro sau 2% din cifra de afaceri globală, precum și afectarea reputației organizației.

Regulamentul privind Reziliența Cibernetică (Cyber Resilience Act)

Adoptat în anul 2024, CRA introduce cerințe obligatorii de securitate pentru toate produsele cu elemente digitale comercializate în UE. Dacă NIS2 se concentrează pe operatorii de servicii și infrastructuri critice, CRA vizează producătorii și dezvoltatorii, asigurând integrarea securității „by design" și „by default" încă din faza de proiectare[15]. Cerințele minime presupun dezvoltarea securizată a produselor, remedierea vulnerabilităților înainte de lansare, furnizarea de actualizări sigure, protecția datelor utilizatorilor, furnizarea unei configurații securizate implicit, care să fie compatibilă cu utilizarea prevăzută și să poată fi restaurată complet prin intermediul unei funcții de resetare. Producătorii trebuie să monitorizeze permanent vulnerabilitățile, să raporteze incidentele majore autorităților competente (ENISA sau cele naționale) și să informeze utilizatorii afectați.

Pentru IMM-urile românești, CRA va avea un impact direct: regulamentul, publicat în Jurnalul Oficial al Uniunii Europene la 20 noiembrie 2024, se va aplica automat după o perioadă de tranziție de trei ani, adică din decembrie 2027, impunând standarde riguroase care pot deveni un avantaj competitiv. Respectarea acestor cerințe demonstrează conformitatea cu principiile de securitate „by design", reducând riscurile din LAS încă din etapa de dezvoltare și consolidând încrederea clienților și a partenerilor de afaceri[16].

Figura 3. Comparație între CRA și NIS2

În ansamblu, aceste reglementări (Figura 3) definesc o nouă etapă a securității cibernetice europene, în care protecția lanțului de aprovizionare software devine o condiție esențială pentru reziliența digitală și pentru menținerea competitivității economice la nivelul Uniunii Europene.

[15]https://www.securebydesignhandbook.com/docs/standards/eu/cra-overview
[16]https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity

Studii realizate de ENISA

ENISA joacă un rol central în eforturile de îmbunătățire a securității lanțului de aprovizionare digital la nivel european. ENISA acționează atât ca organism de expertiză, elaborând ghiduri de bune practici și analize de amenințări, cât și ca facilitator al implementării noilor reglementări (precum NIS2 și CRA) prin recomandări și instrumente dedicate.

În anul 2021, ENISA a publicat primul raport special dedicat *amenințărilor lanțului de aprovizionare* (Threat Landscape for Supply Chain Attacks)[17], care a analizat tendințele și modurile de operare din 24 de incidente semnificative. Concluziile au evidențiat creșterea frecvenței acestor atacuri și faptul că o organizație poate fi vulnerabilă chiar dacă are măsuri de securitate interne adecvate, deoarece adversarii exploatează relația de încredere cu furnizorii. Raportul ENISA (Figura 4) a evidențiat faptul că **62%** dintre

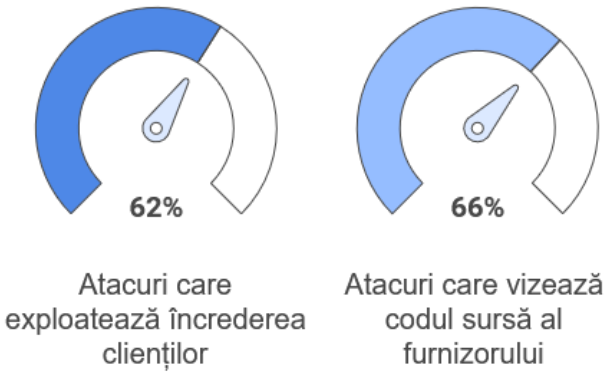

Figura 4. Vectori de atac conform ENISA

atacuri au profitat de nivelul de încredere pe care clienții îl acordă furnizorului compromis și că, în **66%** din cazuri, atacatorii au vizat direct codul sursă al furnizorului pentru a-și atinge scopul. Aceste informații i-au determinat pe factorii de decizie europeni să introducă cerințe privind securitatea LAS în Directiva NIS2 și să propună măsuri, precum Regulamentul CRA, pentru creșterea protecției produselor digitale.

Ulterior, în anul 2023, ENISA a realizat un **studiu privind practicile curente de securitate a lanțului de aprovizionare** în rândul organizațiilor europene esențiale și importante, publicând un raport de bune practici - „Good Practices for Supply Chain Cybersecurity"[18]. Acest raport sintetizează atât constatările studiului (privind nivelul de pregătire actual al organizațiilor, alocarea bugetelor pentru securizarea lanțului de aprovizionare etc.), cât și un set de măsuri recomandate, extrase din standarde internaționale.

Studiul arată că, deși 86% dintre organizații aveau politici privind securitatea lanțului de aprovizionare TIC, 76% nu stabiliseră cine este efectiv responsabil pentru aplicarea lor. Doar 47% alocau buget specializat, 61% solicitau certificări de securitate furnizorilor, 43% utilizau servicii externe de evaluare, iar 37% realizau analize proprii. Doar 9% au indicat că nu efectuează nicio formă de evaluare. Aceste cifre denotă o conștientizare în creștere, dar și lacune, de exemplu, lipsa personalului dedicat. ENISA recomandă organizațiilor, indiferent de mărime, să creeze un **sistem, la nivel de companie pentru managementul lanțului de aprovizionare**, integrat în cadrul de management mai larg al riscului terților părți (Third-Party Risk Management). Un asemenea sistem ar trebui să acopere: evaluarea riscurilor LAS, managementul relațiilor cu furnizorii, managementul vulnerabilităților și asigurarea calității și securității produselor de la furnizori pe tot parcursul ciclului lor de viață.

Pentru a sprijini în special IMM-urile, ENISA a lansat, în anul 2021, inițiativa **SecureSME**[19], un portal care oferă recomandări personalizate, orientări practice și resurse de conștientizare adaptate nevoilor IMM-urilor. Ideea promovată de ENISA este că securitatea cibernetică *poate fi eficientă fără costuri ridicate* pentru IMM. Multe măsuri țin de bună guvernanță, configurări corecte și instruirea personalului, lucruri

[17]https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%20for%20Supply%20Chain%20Attacks.pdf
[18] https://www.enisa.europa.eu/sites/default/files/publications/Good Practices for Supply Chain Cybersecurity.pdf
[19] https://www.enisa.europa.eu/tools/securesme

care pot fi realizate cu investiții minime. Prin această platformă, IMM-urile pot accesa liste de verificare, ghiduri de bune practici și instrumente gratuite care să le ajute să-și evalueze nivelul de pregătire și să implementeze îmbunătățiri.

Măsuri recomandate pentru IMM-uri

Gestionarea riscurilor necesită o abordare multidimensională, care îmbină guvernanța, controalele tehnice și procese/politici clar definite. Ghidul propune măsuri etapizate, adaptate IMM-urilor, derivate din standarde și bune practici europene și internaționale. Securitatea lanțului de aprovizionare este un proces continuu de evaluare și îmbunătățire care trebuie integrat în cultura organizațională.

Guvernanță și cultura securității

Securitatea lanțului de aprovizionare nu depinde exclusiv de soluțiile tehnice, ci este susținută de implicarea conducerii, politici clare, procese bine definite și o cultură a responsabilității comune. O abordare eficientă pornește de la angajamentul managementului și se extinde către fiecare angajat și partener implicați în ecosistemul digital al organizației (Figura 5).

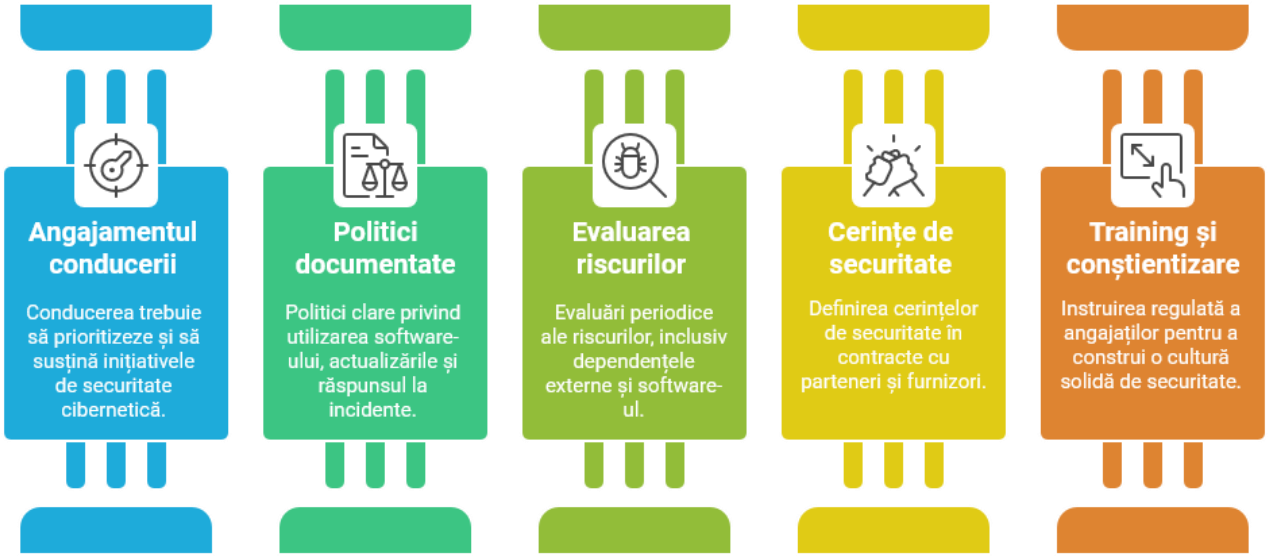

Figura 5. Guvernanță și cultura securității

Astfel, elementele de guvernanță și cultură a securității trebuie consolidate prin măsuri coerente și aplicate sistematic, cum ar fi:

- **Angajament din partea conducerii -** echipa de management trebuie să trateze securitatea cibernetică, inclusiv cea din lanțul de aprovizionare, ca pe o prioritate strategică. Conducerea trebuie să desemneze un responsabil pentru securitate, să aloce resurse și să susțină activ inițiativele din acest domeniu. Chiar și în lipsa unui departament specializat, această funcție poate fi preluată de un manager existent (ex. IT), completată de consultanță externă periodică;

- **Politici și proceduri documentate -** compania trebuie să dețină politici clare privind utilizarea software-ului terț și a actualizărilor, gestionarea vulnerabilităților și evaluarea furnizorilor. În plus, este recomandată elaborarea unui plan de răspuns la incidente cibernetice care să includă scenarii de compromitere a unui furnizor, roluri clare și măsuri de comunicare. DNSC recomandă implicarea furnizorilor critici în exercițiile de răspuns la incidente cibernetice și cooperarea cu aceștia în caz de incident;

- **Evaluarea periodică a riscurilor -** evaluările trebuie să acopere nu doar dependențele externe și componentele software esențiale utilizate în interiorul organizației, ci și servicii, aplicații sau integrări furnizate de terți. Riscurile generate de utilizarea bibliotecilor open-source sau de relațiile cu furnizorii trebuie identificate și tratate prin măsuri adecvate – precum monitorizarea continuă, aplicarea promptă a actualizărilor sau înlocuirea cu soluții mai sigure. ENISA recomandă integrarea acestor activități în cadrul mai larg de management al riscurilor terților;

- **Cerințe de securitate pentru parteneri și furnizori -** o guvernanță eficientă presupune definirea clară a cerințelor de securitate în contracte: notificarea incidentelor, audituri, standarde minime de securitate (ex. ISO/IEC 27001). Încrederea se construiește prin responsabilități contractuale clare. Tot mai multe companii solicită furnizorilor **certificări sau dovezi concrete privind nivelul de securitate**, motiv pentru care IMM-urile trebuie să fie pregătite **atât să prezinte, cât și să solicite** astfel de garanții partenerilor lor;

- **Training și conștientizare -** o cultură solidă de securitate se construiește prin instruirea periodică a angajaților. Personalul tehnic trebuie să cunoască riscurile componentelor nevalidate, iar echipele non-tehnice implicațiile contractuale și operaționale.

Controale tehnice de securitate pentru protecția LAS

Controalele tehnice de securitate au rolul de a preveni introducerea de componente compromise, detectarea timpurie a anomaliilor și menținerea continuității activității în caz de incident (Figura 6). Implementarea acestor măsuri trebuie ajustată în funcție de dimensiunea și particularitățile fiecărei organizații, pentru a asigura un nivel de protecție adecvat riscurilor.

Figura 6. Controale de securitate

1) **Inventarierea dependențelor și a activelor**

Obiectiv: identificarea completă a componentelor software (biblioteci, module, dependențe) și a activelor software (aplicații, servicii și sisteme utilizate).

Descriere: inventarierea include toate elementele software folosite de organizație, atât dezvoltate intern, cât și furnizate de terți: biblioteci, pachete, containere, servicii cloud sau framework-uri.

Practică recomandată: generarea unei **Liste de materiale software** (Software Bill of Materials – SBOM) pentru fiecare aplicație. Aceasta reprezintă un document detaliat cu bibliotecile software și versiunile lor, în formate standardizate precum CycloneDX sau SPDX.

Beneficii: permite identificarea rapidă a aplicațiilor afectate de o vulnerabilitate critică (exemplu: Log4Shell din Log4j) și sprijină prioritizarea sistemelor critice în planurile de protecție.

2) Controlul surselor de aprovizionare software

Obiectiv: limitarea riscului de introducere a componentelor compromise.

Descriere: sursele de software și actualizări trebuie definite clar pentru a evita descărcarea necontrolată de componente din medii nesigure. Este recomandată folosirea exclusivă a canalelor oficiale și de încredere (precum site-urile producătorilor, registrele publice verificate) și magazinele de aplicații cu reputație confirmată, precum și restricționarea accesului la surse neautorizate prin politici interne clare.

Măsuri suplimentare: stabilirea unei versiuni fixe (așa-numitul *version pinning*), verificate și aprobate a unei biblioteci, efectuarea unui audit minimal pentru componentele critice și monitorizarea anunțurilor de securitate ale furnizorilor prin buletine dedicate.

3) Verificarea integrității și autenticității

Obiectiv: garantarea faptului că pachetele software provin de la surse legitime și nu au fost modificate.

Descriere: practicile recomandate includ verificarea semnăturilor digitale și a hash-urilor la instalare, utilizarea protocolului HTTPS/TLS și validarea integrității modulelor la momentul încărcării.

Tehnologie emergentă: Sigstore, prin instrumentul său Cosign[20], oferă posibilitatea semnării containerelor, fișierelor executabile și pachetelor software, iar certificatele rezultate sunt stocate într-un registru public, ceea ce permite verificarea originii și autenticității acestora.

4) Actualizarea și gestionarea patch-urilor

Obiectiv: reducerea expunerii la vulnerabilitățile cunoscute.

Descriere: gestionarea riguroasă a actualizărilor presupune monitorizarea permanentă a patch-urilor, testarea și aplicarea lor într-un interval rezonabil. Procesul trebuie să vizeze atât produsele comerciale (sisteme de operare, aplicații standard), cât și componentele din surse deschise integrate în aplicațiile dezvoltate intern.

Exemplu: vulnerabilitatea Log4Shell a evidențiat provocările întâmpinate de organizațiile fără un inventar complet al dependențelor, care nu au reușit să identifice și să remedieze rapid toate instanțele afectate.

5) Izolarea și principiul minimului privilegiu

Obiectiv: limitarea impactului potențial al compromiterii unei componente software.

Descriere: configurarea aplicațiilor externe sau a codului provenit de la terți pentru a rula cu privilegii minime, preferabil în medii izolate (containere, mașini virtuale). În cazul serviciilor cloud sau SaaS, accesul la rețeaua internă trebuie restricționat strict la resursele necesare.

Practică suplimentară: segmentarea rețelei, prin separarea stațiilor de lucru ale dezvoltatorilor de serverele critice și aplicarea principiilor „zero trust", prin verificări și restricții la fiecare nivel de acces.

6) Monitorizarea și detecția anomaliilor

Obiectiv: identificarea timpurie a comportamentelor suspecte ce pot indica un atac.

Descriere: mecanismele eficiente includ centralizarea jurnalelor, definirea regulilor de alertare, utilizarea măsurilor de protecție pentru echipamentele **finale** (stații de lucru, laptopuri, telefoane mobile), pentru infrastructura critică (servere, servicii cloud, sisteme de dezvoltare) și monitorizarea permanentă a integrității fișierelor.

[20] https://docs.sigstore.dev/

Context suplimentar: în cazul organizațiilor care dezvoltă software, fluxurile de integrare continuă ar trebui să mențină jurnale detaliate ale proceselor rulate, să valideze semnăturile rezultatelor și să supravegheze orice modificare neautorizată apărută în procesul de compilare și livrare.

7) Copii de siguranță offline și plan de continuitate

Obiectiv: asigurarea rezilienței și continuității activității după un incident sever.

Descriere: practicile recomandate includ menținerea unor copii actualizate ale datelor critice, stocate offline sau în medii izolate, precum și testarea periodică a procedurilor de restaurare.

Măsuri adiționale: Utilizarea copiilor de siguranță „reci" (deconectate după realizare) sau stocate pe suporturi care nu permit modificarea ulterioară a datelor, precum și elaborarea unui plan de continuitate a activității care să includă scenarii precum indisponibilitatea unei aplicații furnizate de un terț.

Procese și politici de gestionare a riscurilor

Gestionarea riscurilor din LAS nu se limitează la măsuri tehnice, ci presupune existența unor procese și politici bine definite, aplicate consecvent la nivel organizațional. Pentru IMM-uri, aceste procese oferă un cadru de acțiune care asigură coerență, trasabilitate și capacitatea de reacție în fața incidentelor. Scopul lor este de a gestiona vulnerabilitățile prin evaluări sistematice, controale administrative (politici, proceduri și responsabilități clare) și colaborare constantă cu partenerii. Implementarea acestor politici contribuie la reducerea riscului de compromitere și la creșterea încrederii în relațiile din lanțul digital.

Figura 7. Implementare măsuri de securitate

Aceste principii pot fi aplicate practic printr-un set de procese operaționale esențiale, pe care IMM-urile le pot adapta (Figura7) în funcție de nivelul de risc și de specificul activității lor:

- **Evaluarea și aprobarea furnizorilor -** înainte de a începe colaborarea cu un nou furnizor de software sau servicii IT, IMM-urile ar trebui să efectueze o **evaluare de securitate** proporțională cu riscurile implicate. Aceasta poate lua forma unui chestionar de securitate privind practicile furnizorului (securitate, certificări, istoric de incidente, conformitate cu NIS2/GDPR etc.), a unei cercetări din surse deschise (căutare de eventuale incidente din trecut, reputație, recenzii) sau chiar a unui audit de securitate (pentru furnizori critici, cu acordul lor). Scopul este identificarea eventualelor puncte slabe înainte de a semna contractul. Un concept util este *clasificarea furnizorilor* în funcție de nivelul de risc (critici, importanți, obișnuiți) și aplicarea unor controale graduale.

De exemplu, pentru furnizorii critici se recomandă semnarea unui acord privind nivelul serviciilor furnizate (Service Level Agreement, SLA) care include aspecte de securitate și se reevaluează performanța lor, pe când pentru furnizori mai puțin importanți aceste cerințe sunt simplificate.

- **Managementul schimbărilor în LAS -** odată ce un furnizor sau produs software a fost aprobat și introdus în ecosistem, organizația trebuie să mențină un **proces de gestionare a schimbărilor**. Este esențial ca organizația să dețină în permanență o imagine clară asupra lanțului de aprovizionare: să cunoască furnizorii, accesul la informații și locul stocării acestora, pentru a reacționa rapid la orice schimbare ce poate afecta securitatea.

- **Colaborare și partajare de informații -** securitatea lanțului de aprovizionare nu poate fi asigurată individual, ci necesită cooperare între organizații. IMM-urile pot câștiga mult prin participarea la platforme de schimb de informații despre amenințări, cum ar fi grupurile sectoriale ISAC (Information Sharing and Analysis Centers - centre de analiză și partajare a informațiilor) sau comunitățile locale de securitate cibernetică. Instituții precum DNSC și Centrul Național CYBERINT publică periodic rapoarte și alerte despre campanii active, inclusiv atacuri pe lanțul de aprovizionare, precum și indicatori de compromitere ce pot fi folosiți în verificările interne. Dacă un IMM constată că a fost afectat, este important să informeze partenerii și autoritățile competente, pentru a limita răspândirea atacului și a sprijini un răspuns coordonat. Directiva NIS2 promovează tocmai această transparență, prin obligațiile de raportare a incidentelor.

- **Planificarea continuității afacerii -** pe lângă măsurile tehnice, precum copiile de siguranță, este necesară și elaborarea unui plan de continuitate a activității (Business Continuity Plan, BCP) care să includă scenarii de compromitere a lanțului de aprovizionare. IMM-ul ar trebui să stabilească, pentru fiecare furnizor sau aplicație esențială, ce soluție alternativă are dacă aceasta devine indisponibilă. De exemplu, dacă serviciul de e-mail sau telefonie este afectat, trebuie să existe o soluție temporară de comunicare; dacă un program de contabilitate este compromis, să existe o modalitate provizorie de lucru până la remediere. Aceste planuri ajută compania să își mențină funcționarea în situații de criză și să evite reacțiile haotice. Ele trebuie testate periodic și actualizate ori de câte ori apar schimbări majore în activitate sau furnizori.

- **Audit și îmbunătățire continuă -** IMM-urile ar trebui să efectueze periodic audituri interne sau externe pentru a evalua practicile de securitate, inclusiv cele legate de LAS. Aceste evaluări pot scoate la iveală probleme ascunse, precum utilizarea de aplicații neautorizate sau nerespectarea procedurilor stabilite. De exemplu, auditul poate identifica achiziții de software realizate fără o analiză prealabilă a riscurilor. Rezultatele trebuie urmate de acțiuni concrete: actualizarea politicilor, instruirea angajaților și, dacă este necesar, schimbarea furnizorilor care nu respectă cerințele de securitate. Un proces constant de optimizare presupune analizarea fiecărui incident sau a fiecărei situații evitate, astfel încât lecțiile învățate să reducă riscul repetării lor.

Adoptarea acestor măsuri poate părea dificilă pentru o organizație mică, însă trebuie abordată gradual. În prima etapă pot fi consolidate elementele de bază precum realizarea copiilor de siguranță, aplicarea actualizărilor și utilizarea unui set clar de software aprobat, urmând ca nivelul de maturitate să crească progresiv. Multe dintre aceste acțiuni depind mai mult de disciplină și organizare decât de resurse financiare. După cum subliniază ENISA, securitatea cibernetică nu este neapărat costisitoare pentru IMM-uri, existând numeroase măsuri eficiente ce pot fi implementate fără investiții semnificative[21]. În plus, există o serie de instrumente gratuite sau disponibile la costuri reduse care pot sprijini IMM-urile să adopte și să implementeze controalele de securitate, ce vor fi prezentate ulterior.

Instrumente pentru securitatea LAS

Implementarea măsurilor de securitate poate fi sprijinită prin utilizarea unor instrumente software specializate. Numeroase soluții gratuite sau cu costuri reduse, adesea disponibile pe Internet și dezvoltate de comunitatea de securitate, sunt accesibile IMM-urilor. Acestea se integrează relativ ușor în infrastructura existentă și acoperă o gamă variată de nevoi: inventarierea și scanarea vulnerabilităților, inclusiv din dependențe, auditarea mediilor de dezvoltare și operare precum și semnarea codului. Niciun

[21] https://www.enisa.europa.eu/tools/securesme

instrument nu este suficient de unul singur, însă utilizarea unei suite adecvate, completată de analiză umană, poate automatiza și simplifica semnificativ sarcinile de securitate.

Pentru IMM-urile cu bugete reduse, o soluție practică este combinarea programelor gratuite cu versiunile de bază oferite de unele servicii comerciale. Astfel, se obține o protecție mai bună fără cheltuieli mari. Se pot utiliza programe gratuite pentru verificarea bibliotecilor folosite, unelte simple pentru semnarea aplicațiilor și a serviciilor gratuite de monitorizare.

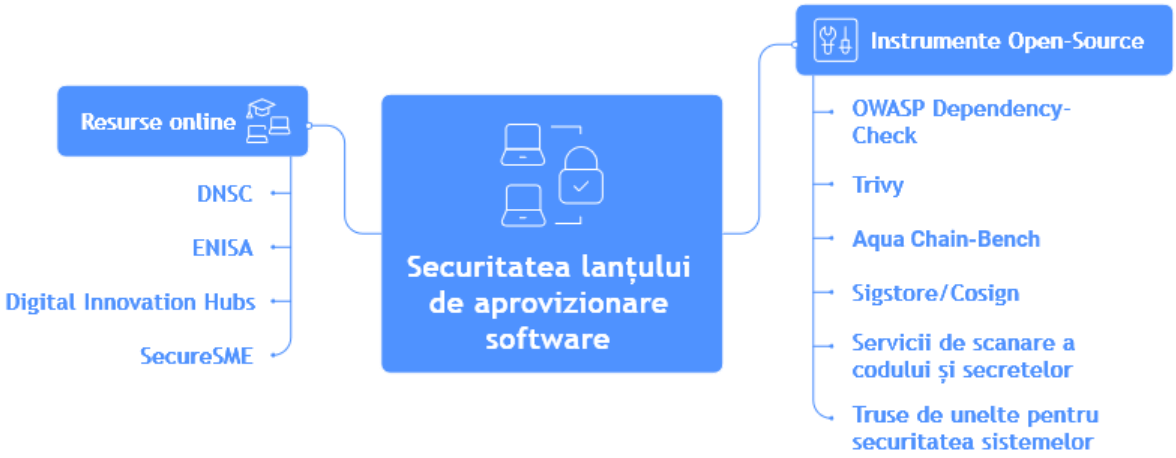

Figura 8. Resurse de securitate pe lanțul de aprovizionare

În continuare este prezentată o listă de instrumente utile (Figura 8), grupate pe categorii, care pot ajuta la reducerea riscurilor din lanțul de aprovizionare software:

- **OWASP Dependency-Check -** este un instrument care analizează proiectele software pentru a identifica bibliotecile utilizate și vulnerabilitățile cunoscute asociate acestora. Suportă mai multe limbaje de programare și utilizează baza de date NVD. La final, generează un raport ce permite actualizarea sau corectarea componentelor afectate. O alternativă complementară este **OWASP Dependency-Track**, care oferă și o gestiune centralizată a componentelor și a listelor SBOM.

- **Trivy -** instrument open-source dezvoltat de Aqua Security, utilizat pentru scanarea vulnerabilităților în containere, imagini Docker, pachete software și configurații. Este ușor de folosit și oferă rezultate rapide, identificând vulnerabilitățile raportate în mod public (Common Vulnerabilities and Exposures, CVE) din componentele analizate. Poate fi integrat în procesele de integrare continuă pentru a împiedica distribuirea **pachetelor software** cu probleme critice. În plus, permite generarea de SBOM-uri și verificarea configurațiilor Kubernetes sau Infrastructure as Code (IaC). Prin acoperirea mai multor funcții într-un singur instrument gratuit, Trivy este deosebit de util pentru IMM-urile care utilizează containere sau servicii cloud.

- **Aqua Chain-Bench -** instrument open-source pentru auditul practicilor de securitate din LAS. Evaluează dacă procesele de dezvoltare și livrare respectă standarde recunoscute, precum ghidurile publicate de Center for Internet Security (CIS). Analizează configurațiile din fluxurile automate de construire a aplicațiilor și setările surselor de cod (de exemplu, verificarea modificărilor propuse, scanarea dependențelor sau semnarea imaginilor software) și semnalează eventualele neconformități. Practic, acționează ca o listă automată de verificare care ajută echipele să își îmbunătățească practicile de securitate în procesul de dezvoltare. Pentru IMM-uri, oferă o modalitate simplă și gratuită de a se familiariza cu cerințele de securitate ale lanțului software.[22]

- **Sigstore/Cosign -** soluție open-source pentru semnarea și verificarea artefactelor software, adică a tuturor fișierelor rezultate în procesul de dezvoltare (de exemplu: imagini de containere, binare, biblioteci, scripturi sau pachete instalabile). Cosign permite aplicarea de semnături digitale pentru fișiere și pentru imagini de containere în format standard (Open Container Initiative, OCI), cu posibilitatea de a stoca aceste semnături fie în registrele de containere, fie în jurnale publice de transparență. Pentru IMM-

[22] https://www.aikido.dev/blog/top-software-supply-chain-security-tools

uri, acest mecanism facilitează validarea integrității și a proveniențeі imaginilor sau a scripturilor înainte de utilizare. Pot fi folosite imagini de container semnate de furnizori de încredere, precum Chainguard, care oferă gratuit versiuni „secure-by-design”.

- **Servicii de scanare a codului pentru informații sensibile -** expunerea accidentală a unor informații sensibile, precum chei API (Interfață de Programare a Aplicațiilor) sau parole, reprezintă un risc semnificativ în LAS. Instrumente open-source precum **Gitleaks** sau **TruffleHog** pot scana repository-urile Git pentru a detecta astfel de date. Platforme precum **GitGuardian** oferă gratuit monitorizare limitată pentru **depozitele publice de cod** și transmit alerte atunci când sunt detectate probleme de securitate. Pentru IMM-uri, este esențială integrarea acestor soluții în procesul de verificare a codului și eliminarea rapidă a informațiilor expuse, inclusiv înlocuirea cheilor compromise. În completare, **instrumentele de analiză statică a codului** pot detecta vulnerabilități introduse accidental, prevenind transformarea aplicațiilor proprii într-o potențială sursă de risc pentru clienți.

- **Soluții pentru securitatea sistemelor -** IMM-urile pot implementa instrumente gratuite sau cu cost redus pentru a consolida securitatea operațională de zi cu zi. Exemple includ OpenVAS pentru scanarea vulnerabilităților, Zeek sau Suricata pentru monitorizarea traficului de rețea și OSQuery pentru verificarea configurațiilor și a indicatorilor de atac pe stațiile de lucru. Deși nu sunt dedicate exclusiv lanțului de aprovizionare, aceste instrumente pot detecta efectele unor atacuri indirecte, cum ar fi malware-ul introdus printr-un software aparent legitim. În plus, scanere de integritate precum Tripwire sau AIDE (Advanced Intrusion Detection Environment) semnalează modificarea neautorizată a fișierelor aplicațiilor.

- **Resurse online și platforme de informații -** Deși nu sunt unelte tehnice propriu-zise, IMM-urile pot accesa resurse gratuite de sprijin. **DNSC** publică alerte și ghiduri practice, inclusiv materiale aplicabile IMM-urilor. **ENISA** pune la dispoziție secțiuni dedicate conștientizării și instruirii, iar inițiative europene precum **Digital Innovation Hubs** oferă uneori, evaluări de securitate și programe gratuite de instruire. Un exemplu este platforma **SecureSME**, care centralizează resurse și instrumente pentru a facilita adoptarea de măsuri de securitate de către IMM-uri.

Instrumentele gratuite pot reduce suprafața de atac și pot oferi avertizări timpurii, totuși acestea pot avea funcționalități limitate, suport redus și pot necesita competențe tehnice ridicate pentru configurare, ceea ce poate îngreuna utilizarea lor eficientă. În lipsa acestora, se poate apela la comunitățile de utilizatori sau la consultanți pentru configurarea inițială. Chiar și cu resurse limitate, IMM-urile pot atinge un nivel solid de protecție prin utilizarea eficientă a acestor soluții.

Concluzii

Lanțul de aprovizionare software constituie, în prezent, una dintre principalele provocări ale securității cibernetice, aspect pe care IMM-urile nu îl mai pot neglija. Odată cu accelerarea proceselor de digitalizare și interconectare, protecția cibernetică depășește limitele organizației și trebuie extinsă asupra întregului flux prin care software-ul și serviciile pătrund în infrastructura organizației. Importanța subiectului este evidențiată de creșterea semnificativă a atacurilor pe LAS în ultimii ani, precum și de atenția acordată acestui domeniu prin reglementări europene, precum Directiva NIS2 și Cyber Resilience Act. Totodată, clienții și partenerii de afaceri solicită tot mai frecvent garanții de securitate de-a lungul lanțului de aprovizionare, iar capacitatea unei întreprinderi de a demonstra că este un partener sigur și de încredere poate constitui un avantaj competitiv.

Pentru a face față provocărilor actuale, IMM-urile din România trebuie să adopte o abordare proactivă și structurată a securității. Gestionarea riscurilor din lanțul de aprovizionare necesită un efort integrat, care implică atât conducerea, cât și echipele tehnice și de achiziții, prin colaborare permanentă și o înțelegere comună a responsabilităților.

Cadrul legislativ european aduce atât obligații, cât și oportunități: reglementările precum Directiva NIS2 impun standarde minime de securitate, iar inițiativele ENISA și DNSC oferă sprijin prin ghiduri și instrumente gratuite. Aceste cerințe nu trebuie privite ca o povară administrativă, ci ca o investiție în reziliența și competitivitatea organizației. Un lanț de aprovizionare sigur înseamnă continuitate operațională, reducerea pierderilor și consolidarea încrederii pe piață.

Securitatea absolută nu există, însă prin măsuri tehnice adecvate, organizare și cooperare, IMM-urile își pot reduce considerabil riscurile din LAS. Eforturile trebuie adaptate nivelului de risc, iar securitatea rămâne un proces continuu de prevenire și învățare.

Bibliografie

1. ENISA – Threat Landscape for Supply Chain Attacks 2021, https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%20for%20Supply%20Chain%20Attacks.pdf

2. Codrea, I. & Savin, A.– Strategia & cadrul legal: bazele rezilienței cibernetice pentru IMM-uri (CyberTM 2025)

3. ITAdviser (2025) – Directiva NIS2 – Ghid rapid pentru conformare și securitate cibernetică

4. ENISA (2023) – Good Practices for Supply Chain Cybersecurity https://www.enisa.europa.eu/sites/default/files/publications/Good%20Practices%20for%20Supply%20Chain%20Cybersecurity.pdf

5. ENISA – SecureSME Tool, https://www.enisa.europa.eu/tools/securesme

6. Aqua Security Aikido Blog (2025) – Top Software Supply Chain Security Tools (Free/Open Source)

7. https://digital-strategy.ec.europa.eu/ro/news/enisa-published-its-threat-landscape-supply-chain-attacks

8. https://www.reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05/

9. https://securitatea-cibernetica.ro/documente/Legea-privind-securitatea-si-apararea-cibernetica-a-Romaniei.pdf

10. https://thehackernews.com/2023/02/python-developers-beware-clipper.html

11. https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_5375

12. https://www.aquasec.com/cloud-native-academy/supply-chain-security/sbom-tools/

13. https://www.aikido.dev/blog/top-software-supply-chain-security-tools

14. CISA (2022) - Securing the Software Supply Chain Recommended Practices Guide for Customers and accompanying Fact Sheet https://www.cisa.gov/resources-tools/resources/securing-software-supply-chain-recommended-practices-guide-customers-and

Anexa A - Studii de caz

Pentru a înțelege mai bine modul în care se materializează amenințările lanțului de aprovizionare și ce învățăminte pot fi trase, descriem câteva incidente cibernetice **reale** de referință. Aceste exemple acoperă scenarii diferite de atac și subliniază importanța măsurilor discutate anterior. Fiecare caz este urmat de lecțiile învățate, relevante pentru IMM-uri.

Atacul SolarWinds Orion (2020)

Descriere incident: platforma **SolarWinds Orion** de monitorizare a rețelelor a fost compromisă după ce atacatorii au infiltrat mediul de dezvoltare și au inserat un backdoor numit *SUNBURST* în actualizările software distribuite în perioada martie-iunie 2020. Peste 18.000 de organizații au instalat versiunile infectate, inclusiv agenții guvernamentale și companii din domeniul tehnologic.

Mod de acțiune: backdoor-ul rămânea inactiv o perioadă pentru a evita detecția, apoi se activa, oferind acces la rețelele compromise. Atacatorii comunicau prin canale legitime, ocolind autentificarea și selectând doar ținte de interes. Incidentul a fost descoperit abia după mai multe luni, în urma unei investigații efectuate de compania FireEye.

Lecții învățate:

- aplicarea principiilor Zero Trust, inclusiv față de furnizorii de încredere;
- monitorizarea comportamentală și segmentarea rețelei pot limita impactul unui atac;
- adoptarea practicilor DevSecOps întărește securitatea softului dezvoltat;
- comunicarea transparentă și cooperarea între organizații accelerează remedierea;
- includerea de planuri clare de răspuns la incidente și să acționeze prompt la notificările furnizorilor.

Campania de pachete PyPI malițioase (2022–2023)

Descriere incident: între anii 2022 și 2023, au fost identificate peste 450 de coduri Python malițioase publicate pe registrul oficial PyPI, imitând librării legitime prin tehnica *typosquatting* (ex. marplotlib în loc de matplotlib). Pachetele conțineau malware de tip *clipper*, care înlocuia adresele de portofele crypto din clipboard cu cele ale atacatorilor. Codul malițios instala și o extensie ascunsă de browser pentru persistență.

Mod de acțiune: atacatorii au automatizat procesul de încărcare masivă a pachetelor și au folosit tehnici de camuflare subtilă pentru a păcăli dezvoltatorii. Unele versiuni au modificat scurtăturile browserelor, menținând accesul chiar după restart.

Lecții învățate:

- evitarea instalării manuale a pachetelor și folosirea unui fișier care enumeră dependențele proiectului (de exemplu, requirements.txt);
- implementarea scanărilor automate de vulnerabilități (ex. OWASP Dependency-Check, dep-scan);
- testarea pachetelor noi în medii izolate (VM, containere, sanbox-uri);
- activarea autentificării MFA pentru conturile PyPI și verificarea atentă a surselor;
- politicile de securitate trebuie incluse încă din etapa de dezvoltare (shift-left security).

Atacul ransomware via Kaseya VSA (2021)

Descriere incident: gruparea REvil a exploatat o vulnerabilitate zero-day din platforma Kaseya VSA, utilizată de furnizorii de servicii IT (MSP) pentru administrarea rețelelor clienților. Prin compromiterea serverelor VSA, atacatorii au distribuit o actualizare falsă care a instalat ransomware pe mii de sisteme administrate. În doar câteva ore, sute de companii - în special IMM-uri - au fost paralizate.

Impact: între 800 și 1500 de firme au fost afectate la nivel global, inclusiv un lanț de supermarketuri din Suedia. REvil a cerut o răscumpărare de 70 de milioane de dolari, dar Kaseya a obținut ulterior cheia de decriptare și a sprijinit clienții în recuperarea datelor.

Lecții învățate:

- externalizarea IT nu elimină riscurile - furnizorii trebuie evaluați și monitorizați constant;
- contractele cu MSP-urile trebuie să includă cerințe de securitate (patching rapid, MFA, segmentare);
- comunicarea rapidă și acțiunea imediată pot limita impactul unui atac;
- backup-urile offline sunt esențiale pentru recuperarea datelor;
- încrederea excesivă în furnizori nu înseamnă siguranță;
- fiecare companie trebuie să își gestioneze propriul risc.

Atacul S1ngularity / Nx → npm (2025)

Descriere incident: în data de **26 august 2025**, a fost declanșată campania **„S1ngularity”**, în care atacatorii au exploatat o vulnerabilitate într-un flux automatizat (*workflow*) GitHub Actions din proiectul **Nx**. Prin această breșă, atacatorii au exploatat o slăbiciune dintr-un proces automat al unui proiect software găzduit pe GitHub. Prin această breșă au obținut cheia folosită pentru publicarea actualizărilor acelui proiect și au reușit să distribuie versiuni modificate și periculoase ale software-ului către utilizatori.

Mod de acțiune: fluxul compromis a permis atacatorilor să obțină acces la token-ul de autentificare npm al proiectului, permițând publicarea de versiuni compromise ale pachetelor oficiale.

Lecții învățate (pentru IMM-uri):

- controlul strict al workflow-urilor CI/CD: orice script sau acțiune externă trebuie revizuit și restricționat;
- limitarea privilegiilor și protejarea token-urilor: aceste chei digitale, folosite pentru autentificare și publicare, trebuie păstrate în siguranță, actualizate periodic și configurate cu drepturi minime monitorizare post-publicare: verificarea integrității și controlul versiunilor nou publicate, inclusiv semnături digitale.

Atacul npm - septembrie (2025)

Descriere incident: în data de 8 septembrie 2025, ecosistemul **npm** a suferit un atac major asupra LAS. Atacatorii au compromis conturi de administratori și mentori printr-o campanie de phishing, iar cu accesul obținut au modificat sau publicat peste 200 de pachete aflate în registrul oficial npm.

Mod de acțiune: cu acces la conturile compromise, atacatorii au injectat cod malițios în pachete, afectând milioane de distribuiri. Pachetele infectate au fost distribuite printr-o platformă publică de găzduire a pachetelor software (registry.npmjs.org), de unde utilizatorii le descărcau automat atunci când instalau bibliotecile necesare.

Lecții învățate (pentru IMM-uri):

- protejarea conturilor care au roluri de administrare sau publicare în registrele de pachete prin activarea autentificării cu mai mulți factori (MFA);
- verificarea conținutului pachetelor software, în special la primele versiuni sau după modificări majore, pentru a confirma integritatea și siguranța acestora;
- izolarea mediului de testare: pachetele noi sau modificate să fie testate într-un mediu controlat înainte de includere în producție.

Aceste studii de caz relevă faptul că atacurile asupra lanțului de aprovizionare pot afecta orice tip de organizație, indiferent de mărime sau domeniu. Reziliența în fața acestor amenințări nu se bazează doar pe tehnologii de protecție, ci și pe procese solide de management, planuri de continuitate și cooperare între parteneri. În urma acestor atacuri, companiile au îmbunătățit practicile de dezvoltare securizată, platformele open-source au introdus controale mai stricte, iar nivelul general de conștientizare a crescut. IMM-urile pot învăța din aceste exemple pentru a-și ajusta strategiile de securitate și pentru a preveni situații similare, în loc să reacționeze doar după producerea unui incident.

Anexa B - Termeni și abrevieri

Abrevieri

BCP – *Business Continuity Plan*: plan pentru menținerea activității în criză.

API - *Application Programming Interface***:** protocoale care permit aplicațiilor software să comunice între ele.

CI/CD – *Continuous Integration / Continuous Delivery*: procese automate de integrare, testare și livrare.

CIS – *Center for Internet Security*: ghiduri și reguli de configurare sigură.

CRA – *Cyber Resilience Act*: regulament UE cu cerințe de securitate pentru produse digitale.

CVE – *Common Vulnerabilities and Exposures*: identificatori standard ai vulnerabilităților.

DNSC – Directoratul Național de Securitate Cibernetică (România).

DORA – *Digital Operational Resilience Act*: reziliență operațională în sectorul financiar.

ENISA – Agenția UE pentru Securitate Cibernetică.

GDPR – Regulamentul general privind protecția datelor.

IoC – *Indicator of Compromise*: indicator tehnic al unei compromiteri.

IaC – *Infrastructure as Code*: definirea infrastructurii prin cod.

ISAC – *Information Sharing and Analysis Center*: platformă sectorială de schimb de informații.

LAS – Lanțul de aprovizionare software.

MFA – *Multi-Factor Authentication*: autentificare cu mai mulți factori.

MSP – *Managed Service Provider*: furnizor de servicii IT administrate.

NIS2 – Directiva UE pentru un nivel comun ridicat de securitate cibernetică.

NVD – *National Vulnerability Database*: bază publică de vulnerabilități.

NX - set de unelte folosite de dezvoltatori pentru a organiza și automatiza proiecte software mari.

NPM - magazin online de pachete software folosit de programatori pentru a descărca și instala componente necesare în aplicațiile lor.

OCI – *Open Container Initiative*: standarde pentru imagini de containere.

SAST – *Static Application Security Testing*: analiză statică a codului.

SBOM – *Software Bill of Materials*: listă a componentelor software dintr-o aplicație.

SLA – *Service Level Agreement*: acord privind nivelul serviciilor.

Termeni

Acord privind nivelul serviciilor furnizate (*Service Level Agreement***,** SLA**)** – contract care stabilește parametrii de performanță, disponibilitate și securitate pe care furnizorul se angajează să îi respecte;

Backdoor – mecanism ascuns introdus intenționat sau accidental într-un sistem informatic, care permite obținerea de acces neautorizat, ocolind procedurile de autentificare obișnuite;

Copii „reci" (cold backup) – copii de siguranță realizate și apoi deconectate de la rețea, pentru a preveni modificarea sau compromiterea lor în cazul unui atac cibernetic;

Dependențe indirecte – componente software utilizate prin intermediul altor biblioteci sau module, care pot introduce vulnerabilități fără a fi vizibile direct în proiectul principal;

DevSecOps – abordare care integrează practicile de securitate informatică în toate etapele procesului de dezvoltare și operare a software-ului, promovând colaborarea între echipele de dezvoltare, securitate și operațiuni;

CycloneDX – format standard deschis pentru crearea *listelor de materiale software* (*Software Bill of Materials*, SBOM)

SPDX (Software Package Data Exchange) – standard internațional, susținut de Linux Foundation, utilizat pentru documentarea originii, licențelor și versiunilor componentelor software.

Jurnal de transparență – registru public care înregistrează semnăturile, certificatele sau atestările asociate componentelor software, permițând verificarea originii și autenticității acestora;

Privilegiu minim – regulă de securitate conform căreia utilizatorii, procesele sau aplicațiile primesc doar drepturile strict necesare pentru îndeplinirea sarcinilor lor, reducând astfel riscul de abuz sau exploatare;

Pinning de versiuni – practică prin care se fixează explicit versiunea unei biblioteci software utilizate, pentru a preveni actualizările necontrolate ce pot introduce vulnerabilități;

Registru de pachete – infrastructură publică sau privată destinată stocării și distribuirii bibliotecilor software, de unde dezvoltatorii pot descărca și integra componente în aplicațiile lor;

Typosquatting – tehnică malițioasă ce constă în crearea unor pachete software cu denumiri foarte asemănătoare celor legitime, cu scopul de a induce în eroare dezvoltatorii și de a facilita instalarea de cod malițios;

Zero trust – principiu de securitate conform căruia niciun utilizator, dispozitiv sau aplicație nu este considerat implicit de încredere; fiecare acces este verificat și autorizat individual, indiferent de locația sau statutul sursei.

Autori: Irina NEMOIANU, Dan ANDRIEȘ

TLP:CLEAR se poate folosi atunci când informațiile prezintă un risc minim de utilizare abuzivă, în conformitate cu normele și procedurile aplicabile pentru publicare. Sub rezerva regulilor standard ale drepturilor de autor, informațiile TLP:CLEAR pot fi partajate fără restricții.