AVANTAJELE SECURITĂȚII CIBERNETICE

Deși securitatea cibernetică reprezintă un element foarte important pentru organizații, cele mai multe dintre ele pun la îndoială beneficiile obținerii certificării. În ultima perioadă de timp, au existat multe discuții și eforturi de marketing, centrate pe o gamă largă de certificări de securitate cibernetică, ce promovează procesul de operaționalizare a securității în cadrul organizației.

Avantajele certificării cibernetice:

- îmbunătățirea sistemului de management al companiei;
- îmbunătățirea imaginii companiei în fața clienților;
- controlul și reducerea riscurilor la adresa securității cibernetice;
- organizația este protejată împotriva atacurilor cibenetice;
- valorificarea optimă a oportunităților de pe piață;
- câștigarea încrederii partenerilor de pe piața internă și internațională;
- sunt evitate penalitățile și pierderile financiare asociate cu pierderea datelor;
- aduce îmbunătățiri substanțiale în ceea ce privește protecția datelor personale în conformitate cu cerintele Regulamentul UE privind protecția datelor cu caracter personal (GDPR);
- scoate în evidență o abordare proactivă față de amenințările la adresa securității informațiilor, organizația adoptând cele mai bune practici pentru a minimiza amenințările;
- ajută personalul organizației să migreze de la activități de securitate ad-hoc la practici operaționale holistice și continue, vizibile în mediul intern și extern;
- contribuie la identificarea, managementul și minimizarea amenințărilor care afectează informațiile;
- menține operațiunile și practicile de securitate în prim-plan pentru tot personalul, nu numai pentru echipa IT. Prin urmare, securitatea este responsabilitatea întregii organizații. Procesul de obținere a certificării impune bunele practici și reduce riscurile prin:
  - ✓ Reglementarea revizuirii și evaluării practicilor de securitate
  - ✓ Prioritizarea securității pentru personalul de management, IT și operațiuni
  - ✓ Aplicarea proceselor regulate în afaceri și operațiuni

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

✓ Gestionarea riscului

Pe plan extern, o certificare de securitate cibernetică comunică clienților, furnizorilor și întregului ecosistem de afaceri că organizația are ca prioritate securitatea cibernetică. Multe organizații au început să solicite standarde minime pentru operațiuni de securitate ca parte a contractelor lor de afaceri. Această tendință se extinde, așa că tot mai multe companii vor urma această tendință.

Uniunea Europeană își propune să dezvolte un cadru de scheme de certificare a securității cibernetice care să demonstreze că soluțiile TIC certificate au nivelul potrivit de protecție a securității cibernetice pentru piața digitală europeană. Agenția Uniunii Europene pentru Securitate Cibernetica ENISA elaborează proiecte de scheme de certificare, la cererea Comisiei Europene sau a statelor membre ale UE.

În prezent, 3 scheme de certificare a securității cibernetice sunt în curs de dezvoltare:

- o schemă, care acoperă produsele TIC („EUCC"), care se bazează pe o schemă internațională existentă numită „Criterii comune", în curs de finalizare.
- o schemă care acoperă serviciile cloud („EUCS")
- o schemă pentru rețelele 5G („EU5G").

Schema EUCC poate servi la certificarea multor tipuri diferite de produse TIC generice și specifice sectorului. Ca atare, este mai mult o schemă orizontală. Utilizatorii schemei pot stabili profiluri de protecție pentru a-și exprima cerințele de securitate.

Schema EUCC servește ca succesor al schemelor naționale ale UE care funcționează în temeiul MRA SOG-IS.

Schema EUCC permite îmbunătățirea condițiilor pieței interne și creșterea nivelului de securitate al produselor TIC dedicate securității (de exemplu, firewall-uri, dispozitive de criptare, gateway-uri, dispozitive de semnătură electronică, mijloace de identificare, cum ar fi pașapoartele etc.), precum și orice produs TIC care încorporează o funcționalitate de securitate (adică, routere, smartphone-uri, carduri bancare, dispozitive medicale, tahografe pentru camioane etc.).

Oferă două (2) niveluri de asigurare a securității, „substanțial" și „ridicat" și acoperă o mare varietate de cerințe de securitate exigente, deși nu abordează nivelul de bază care poate fi oferit de schemele care sunt mai puțin solicitante în ceea ce privește dovezile de evaluare.

În ceea ce privește avantajele de luat în considerare pentru selectarea acestei scheme pentru securitatea cibernetică a produselor TIC, unele sunt direct legate de caracteristicile schemei (de exemplu, reutilizarea activităților de certificare, posibilitatea de a stabili Profiluri de Protecție):

- Menținerea certificatelor și monitorizarea conformității au fost dezvoltate pe scară largă pentru schema EUCC pentru a oferi asigurarea că securitatea produsului este menținută.
- Criteriile comune sunt criterii armonizate, recunoscute de comitetele internaționale de standardizare ale ISO și IEC, care sunt menținute în mod continuu de o comunitate europeană și internațională, compusă din reprezentanți tehnici și organizatori, care lucrează împreună cu scopul exclusiv de a îmbunătăți standardul.
- CC furnizează un limbaj (un fel de pseudo-formal) pentru a reprezenta funcțiile de securitate, mecanismele și acțiunile de evaluare a acestora. CC sunt flexibile, deoarece

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

oferă un catalog de familii și funcții și operațiuni pentru a le utiliza și extinde, pentru a descrie orice tip de produs TIC, fie hardware, firmware sau software, sau combinația lor.

- CC au cel mai mare catalog de cerințe funcționale de securitate (SFR) și cerințe de asigurare a securității (SAR) evaluate de colegi și independente de produs, ceea ce le face aplicabile unei game largi de produse TIC.

- CC au permis un catalog bun de cerințe de bază aprobate de industrie prin Profiluri de protecție.
- Pe lângă securitatea unui produs, CC-urile permit verificarea securității site-ului de dezvoltare și a securității procesului de dezvoltare.
- Certificarea conform acestei scheme la niveluri de asigurare „înalte” provine din autorizarea unei agenții guvernamentale.
- Multe țări și utilizatori apreciază certificarea față de CC: CC are o istorie îndelungată în ceea ce privește recunoașterea sa de către cincisprezece (15) țări UE și peste treizeci (30) de țări în total, la nivel federal și guvernamental. În plus, peste 4500 de produse au fost deja certificate CC și utilizate de miliarde de utilizatori din întreaga lume.
- CC permite consumatorilor să aibă o evaluare imparțială a unui produs TIC: o astfel de evaluare este, de asemenea, o evaluare de securitate, deoarece CC includ o analiză și testare a produsului pentru conformitatea cu cerințele de securitate specifice. Acest lucru crește nivelul de încredere al consumatorului și de încredere în securitatea produsului TIC certificat.
- Set flexibil de niveluri de asigurare a evaluării: mai multe niveluri de asigurare sunt definite în CC și au fost mapate cu două niveluri de asigurare ale CSA. Acest lucru permite acoperirea unui număr mare de nevoi de asigurare a securității ale diferitelor piețe, deoarece, cu cât nivelul de asigurare al produsului este mai ridicat, cu atât există mai multe dovezi pentru securitatea acestuia cu o metodă de testare tot mai riguroasă.
- Schema include măsuri specifice pentru a permite recunoașterea promptă a produselor TIC certificate, deoarece include reguli pentru implementarea și utilizarea unui cadru de etichetare dedicat. Un astfel de cadru a fost conceput pentru a promova plasarea produselor certificate atât în interiorul, cât și în afara pieței unice a UE.

Schema de certificare a securității cibernetice a serviciilor de cloud (EUCS) are la bază mai multe surse diferite, prima fiind raportul Grupului de lucru CSP-CERT, care a fost livrat în 2019 și a oferit un cadru de bază pe care a fost dezvoltată schema candidată EUCS sprijină cele trei niveluri de asigurare din CSA: „de bază”, „substanțial” și „ridicat”.

Cerințele de securitate referitoare la serviciile de cloud și la evaluarea acestora, cresc ca nivel în ceea ce privește sfera, rigoarea și profunzimea evaluării. Cerințele de la nivelul „ridicat” sunt la un nivel ridicat, în timp ce cerințele de la nivelul „de bază” definesc o bază minimă acceptabilă pentru securitatea cibernetică în cloud. Această linie de bază este totuși cuprinzătoare, deoarece acoperă toate aspectele majore ale securității în cloud. Furnizorii de servicii cloud de orice dimensiune îl pot folosi pentru a demonstra că au creat un cadru pentru a garanta o anumită securitate a clienților lor. Nivelul „substanțial”, între ele, va servi pentru a proteja afacerile și poate fi nivelul de alegere pentru mulți solicitanți și utilizatorii acestora.

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

Conținutul acestei prezentări este responsabilitatea exclusivă a DNSC, RENAR și EY și nu reflectă neapărat opinia Uniunii Europene.

Avantajele schemei EUCS sunt:

- schemă armonizată la nivel european;
- garanții puternice de calitate prin utilizarea evaluării terților de către organismele acreditate, supravegherea de către autoritățile naționale, iar la nivel înalt, autorizarea de către autoritățile naționale și evaluarea inter-pares între organismele de evaluare a conformității;
- flexibilitatea oferită de trei niveluri de asigurare diferite care acoperă întreaga gamă de asigurări introduse în Cyber Security Act, cu posibilitatea ca un serviciu cloud certificat să treacă la un nivel superior în viitoarele cicluri de evaluare;
- garanții puternice de transparență, cu informații de securitate puse la dispoziția publicului printr-un site web centralizat;
- asigurarea menținută în timp, cu reevaluări periodice, garanții de eficacitate operațională la nivelurile Substanțial și Înalt;
- un cadru de întreținere pentru schema EUCS în sine, aprobat de instituțiile europene și de statele membre, care oferă garanții puternice pentru funcționarea continuă a sistemului;
- integrarea în cadrul european de certificare a securității cibernetice, care va facilita reutilizarea serviciilor cloud certificate EUCS în scheme verticale;
- pentru furnizorii de servicii de cloud EUCS va permite utilizarea a două metodologii de evaluare adaptate nivelurilor de asigurare, concepute pentru a simplifica integrarea acestora cu alte metodologii consacrate precum [ISO17021] sau [ISAE3402], precum și posibilitatea de a utiliza compoziția pentru a simplifica certificarea serviciilor cloud care se bazează pe alte servicii cloud deja certificate, oferind un certificat care poate fi utilizat pentru a demonstra că serviciul lor cloud îndeplinește cerințele schemei;
- EUCS stabilește cerințe care impun transparență cu privire la împărțirea responsabilității între furnizorii de servicii de cloud și clienții serviciilor de cloud în ceea ce privește securitatea, precum și cerințe care impun transparență cu privire la locația prelucrării și stocării datelor și cu privire la legile aplicabile;
- pentru clienții serviciilor de cloud, EUCS oferă posibilitatea de a utiliza compoziția pentru a-și certifica propriul serviciu cloud atunci când este necesar.
- Pentru autoritățile de reglementare EUCS oferă cerințe care impun transparență cu privire la locația prelucrării și stocării datelor și cu privire la legile aplicabile.

Cu cât procesul de digitalizare devine o caracteristică a societății actuale, cu atât mai mare este expunerea la amenințări cibernetice și riscul de atacuri ciberbetice este în creștere. Acest risc constant erodează încrederea publicului în dispozitive digitale, făcând în același timp mai problematic introducerea progresului digital în viața oamenilor. Acesta este motivul principal pentru care Uniunea Europeană adoptă un întreg set de reglementări comunitare pentru a face piața unică comună digitală mai sigură din punct de vedere cibernetic, mai rezistentă, mai predictibilă și autonomă din punct de vedere strategic. Una dintre măsurile cheie implementate pentru atingerea acestor obiective este certificarea de securitate cibernetică a produselor TIC, servicii și procese, create de UE Cyber Security Act din 2019. Acest program de lucru, încă în curs de

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

desfășurare este implementat printr-un cadru de 3 scheme dar se așteaptă ca și alte domenii inovatoare cheie și priorități strategice să fie identificate și reglementate în viitor.

Sub îndrumarea strategică a Comisiei și controlul tehnic al Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA), Cybersecurity Framework este încă voluntară, cu așteptarea de a deveni o reglementare obligatorie după o perioadă de probă de patru ani, care se încheie la 31 decembrie 2023 și o evaluare pozitivă a Comisiei.

Evaluarea securității cibernetice prin certificare implică și o îmbunătățire din punct de vedere organizațional și socio-cultural, datorită faptul că în zilele noastre securitatea cibernetică nu mai este considerată doar un sector anexă al proceselor economice, ci devine un nou mod de gândire și proiectare de produse, servicii și procese industriale TIC sigure din punct de vedere cibernetic.

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene