***Tratarea Incidentelor de Securitate***

A elaborat: st. Cebotari Dan

A verificat: lect. univ. Bulai Rodica

Conținut

[Scopul și utilizatorii 3](#_Toc118977057)

[Documente de referință 4](#_Toc118977058)

[Terminologia de bază de securitate a informațiilor 4](#_Toc118977059)

[Reguli de utilizare 5](#_Toc118977060)

[Măsuri de tratare 5](#_Toc118977061)

[Anexa 6](#_Toc118977062)

**Scopul și utilizatorii**

Scopul acestui document este de a defini metodologia de evaluare și tratare a riscurilor informaționale în organizatii și de a defini nivelul acceptabil de risc conform standardului ISO/IEC 27001.

Un plan de răspuns la incident este de obicei un set documentat de instrucțiuni cu mai multe faze. Planul de răspuns la incident definește toate acțiunile necesare și subliniază clar responsabilitățile. Este dovedit că constă din mai multe faze. Sunt necesare revizuiri regulate ale unui astfel de plan de management al incidentelor.

Companiile sunt atacate în mod regulat de infractorii cibernetici și suferă adesea daune pe termen lung. Cu o frecvență tot mai mare.

Trăim vremuri tulburi, în continuă schimbare. Lumea este conectată în rețea și digitalizarea avansează. Am experimentat acest lucru foarte clar în 2022, în special, când tot mai mulți oameni și-au mutat locul de muncă într-un birou de acasă. S-au mutat de la o rețea administrată de profesioniști IT la un loc de muncă fără firewall-uri corporative și posibil fără programe antivirus profesionale care să îi protejeze.

Această situație face ca afacerile să fie o rață de ședere pentru infractorii cibernetici și reprezintă provocări majore pentru departamentele IT.

Cu toate acestea, securitatea IT nu este doar preocuparea specialiștilor în securitate; este, de asemenea, responsabilitatea fiecărui angajat. Sarcini aparent simple, cum ar fi:

- Schimbarea parolelor în mod regulat,

- Partajarea informațiilor confidențiale numai cu surse cunoscute și verificate

- Actualizare software,

- Sa facă în mod regulat copii de siguranță ale datelor și

- Folosind în mod constant o strategie de birou/desktop curată

reprezintă o bază importantă pentru o muncă sigură. Ar trebui profitată de orice ocazie pentru a sensibiliza în mod repetat angajații la acest subiect.

Sarcina operatorului de incident este de a limita și atenua incidentul de securitate. Pentru a face acest lucru, el sau ea planifică, gestionează, coordonează activități, precum și comunică cu alți profesioniști în securitate cibernetică. Responsabilii de incidente stabilesc, testează și verifică canalele de comunicare și le comunică personalului corespunzător.

Aceasta este o necesitate pentru a asigura fluxul adecvat al sarcinilor și comunicațiilor.

De asemenea, se asigură că toate cele mai bune practici de tratare a incidentelor și răspuns, standardele, cadrele de securitate cibernetică, legile și reglementările sunt respectate și estimează costurile pe care le poate suporta un incident.

**Documente de referință**

* Registrul de stat al incidentelor de securitate cibernetică
* NIST Cybersecurity Framework.
* Data Processing Agreement;
* Security Incidents
* Security Incident Management
* Statement of Applicability

**Terminologia de bază de securitate a informațiilor**

**Gestionarea incidentelor -** este un plan de acțiune pentru abordarea intruziunilor, furtului cibernetic, refuzul serviciului, incendii, inundații și alte evenimente legate de securitate. Este compus dintr-un proces în șase etape: pregătire, identificare, izolare, eradicare, recuperare și lecții învățate.

**Incident -** Un incident ca eveniment advers de rețea într-un sistem de informații sau rețea sau amenințarea cu apariția unui astfel de eveniment.

**Auditul -** este strângerea de informații și analizarea activelor pentru a asigura lucruri precum respectarea politicilor și securitatea împotriva vulnerabilităților.

**Reguli de utilizare**

* Reducerea frecvenței incidentelor prin securizarea eficientă a rețelelor, sistemelor și aplicațiilor.
* Documentarea directoarelor pentru interacțiunile cu alte organizații cu privire la incidente. Deoarece aceste comunicări adesea trebuie să aibă loc rapid, organizațiile ar trebui să predetermine liniile directoare de comunicare, astfel încât doar informațiile adecvate să fie partajate cu părțile potrivite.
* Orice angajat al organizatiei are obligatia de informa imediat RSI privind orice incident sau eveniment care afecteaza negativ confidentialitatea, interigatea si diponibilitatea informatiei sau care poate crea prejudicii organizatiei.
* In situatia in care un incident de securitate este cauzat de partenerii organizatiei, in functie de cauza si impactul incidentului se poate ajunge la incetarea relatiilor de colaborare.

**Măsuri de tratare**

1. **Pregătirea**Furnizarea instrumentelor și proceselor de gestionare a incidentelor.
2. **Analiză și Identificare**  
   Decizia dacă a avut loc un incident de securitate.
3. **Izolare**  
   Limitarea răspândirii incidentului și prevenirea daunelor ulterioare.
4. **Eradicarea**  
   Programele malware sunt eliminate.
5. **Recuperare**  
   Sistemele și dispozitivele sunt reactivate și devin productive.

**Anexa**

[**https://www.bankinfosecurity.com/6-steps-to-handle-security-incidents-a-5026**](https://www.bankinfosecurity.com/6-steps-to-handle-security-incidents-a-5026)

[**https://otrs.com/otrs-solutions/corporate-security/security-incident-management/**](https://otrs.com/otrs-solutions/corporate-security/security-incident-management/)