DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

7 PRINCIPII STRATEGICE DE SECURITATE CIBERNETICĂ PENTRU MANAGEMENTUL ORGANIZAȚIEI

TLP:CLEAR

Cuprins

Cuvânt înainte

Navigând prin peisajul digital vast și în continuă expansiune, unde tehnologiile evoluează cu o viteză amețitoare și o mare parte din viața noastră se petrece online, ne confruntăm cu o provocare constantă: securitatea cibernetică. Într-o eră a titlurilor clickbait și a dezinformarii pe rețelele sociale, este mai ușor ca niciodată să cădem pradă amenințărilor online.

Scutul invizibil care ne protejează identitatea digitală, informațiile personale și chiar bunăstarea financiară nu mai este doar responsabilitatea departamentului IT. Securitatea cibernetică a devenit o misiune care ne unește pe toți, de la noii angajați la conducerea de top, indiferent de sectorul public sau privat în care activăm.

Vă recomand cu entuziasm acest ghid, care subliniază importanța implicării active a conducerii în identificarea și evaluarea riscurilor cibernetice, asumându-și responsabilitatea la cel mai înalt nivel al organizației. Este esențial ca fiecare lider să își înțeleagă rolul și responsabilitățile în domeniul securității cibernetice, care nu este doar o linie de apărare, ci și un avantaj competitiv major ce previne pierderile financiare semnificative.

Ca lideri, avem o responsabilitate majoră în a cultiva o cultură organizațională sănătoasă, unde securitatea informației este protejată, promovată și valorizată. Atragerea și reținerea specialiștilor în domeniu este esențială. Conducerea, împreună cu angajații, trebuie să asigure respectarea cerințelor legale și să mențină continuitatea activității, chiar și în fața amenințărilor cibernetice.

Acest ghid prezintă șapte principii de securitate cibernetică, care sunt elemente fundamentale ale unei strategii robuste, durabile și adaptabile nevoilor organizaționale.

De peste 27 de ani, am promovat principii de bază ale securității cibernetice și am implementat măsuri de securitate menite să consolideze mediile digitale interoperabile ale administrațiilor publice. Vă recomand să parcurgeți cu atenție acest ghid și să integrați principiile sale în practicile zilnice ale companiei dumneavoastră. Recomandați-l mai departe prietenilor și partenerilor de afaceri. Împreună, vom construi structuri și medii de afaceri rezistente la amenințările actuale.

Liliana Mușețan

LILIANA MUȘEȚAN

Șef al Unității de Securitate Cibernetică

Secretariatul General al Consiliului Uniunii Europene

Introducere

Într-o lume interconectată, unde dependența de tehnologie și date digitale crește constant, securitatea cibernetică devine esențială pentru strategia oricărei organizații. Transformarea digitală aduce oportunități semnificative de creștere și eficiență, dar expune organizațiile la riscuri cibernetice variate și complexe. Astfel, managementul trebuie să adopte o viziune proactivă și integrată asupra securității cibernetice, integrând-o în cultura și strategia de business.

Rapoartele recente ale companiilor PwC[1] și Deloitte[2] indică o creștere alarmantă a incidentelor de securitate cibernetică și a impactului devastator al acestora asupra organizațiilor de toate dimensiunile. Această realitate subliniază necesitatea unei schimbări fundamentale în abordarea securității cibernetice, transformând-o dintr-o problemă tehnică într-o prioritate strategică de business.

Pentru a îmbunătăți securitatea cibernetică a organizației, acest ghid oferă resurse valoroase, metodologii de referință și instrumente practice, precum și întrebări esențiale pentru evaluarea stării actuale de securitate cibernetică. Este crucial să se găsească un echilibru între aspirațiile de creștere și necesitatea de a menține organizația protejată împotriva amenințărilor cibernetice.

Situația globală și cea a întreprinderilor mici și mijlocii (IMM-uri) evidențiază o creștere a sofisticării și intensității atacurilor cibernetice, vizând organizații de toate dimensiunile. Aceasta accentuează necesitatea de a echilibra creșterea cu măsuri eficiente de securitate cibernetică pentru a asigura prosperitatea și sustenabilitatea pe termen lung.

Acest ghid este un punct de plecare esențial pentru managementul organizațiilor, care trebuie să își asume un rol activ în gestionarea securității cibernetice. Prin adoptarea practicilor prezentate, managementul poate transforma securitatea cibernetică într-o oportunitate strategică, consolidând astfel reziliența și competitivitatea organizației în era digitală.

Securitatea cibernetică trebuie să fie integrată în strategia de dezvoltare a fiecărei organizații. Transformarea digitală deschide porțile către eficiență și inovație, dar expune organizațiile la riscuri cibernetice diverse, care necesită o gestionare atentă și proactivă. Acest ghid oferă instrumentele necesare pentru a naviga acest peisaj complex și pentru a transforma securitatea cibernetică într-un avantaj competitiv.

Cele șapte principii de securitate cibernetică descrise în acest material detaliază responsabilitățile fiecărui nivel din organizație și oferă resurse valoroase, metodologii de referință și unelte practice pentru implementare. De asemenea, sunt incluse întrebări fundamentale pentru evaluarea stadiului actual de securitate cibernetică și formularea unei strategii eficiente de prevenire și răspuns la incidente.

Directoratul Național de Securitate Cibernetică recomandă ca managementul organizațiilor să adopte o abordare integrată și proactivă, folosind resursele și recomandările oferite în acest ghid pentru a naviga cu succes în peisajul complex al amenințărilor cibernetice.

[1] Global Risk Survey 2023 | PwC

[2] Cyber Considerations for C-Suite |Deloitte

1.Securitatea cibernetică nu este doar responsabilitatea departamentului IT

Securitatea cibernetică, în calitate de componentă esențială a infrastructurii oricărei organizații moderne, nu se mai limitează doar la responsabilitățile departamentului IT.

Astăzi, securitatea cibernetică este o componentă esențială în strategiile de business, arhitectura sistemelor, dezvoltarea de produse și servicii, și chiar în elaborarea politicilor publice. Aceasta necesită o abordare multidisciplinară și colaborarea strânsă a tuturor departamentelor unei organizații, de la resurse umane până la marketing și managementul de top. Sensibilizarea și formarea tuturor angajaților cu privire la practicile de securitate cibernetică sunt esențiale pentru a construi o cultură organizațională robustă și a proteja activele și datele companiei.

Fiecare angajat, indiferent de poziția sau departamentul său, trebuie să fie conștient de importanța protejării resurselor digitale și să acționeze corespunzător. Departamentul IT joacă un rol central în implementarea tehnică și monitorizarea sistemelor de securitate, dar siguranța informațională este un obiectiv care trebuie împărtășit de întreaga organizație.

Liderii companiilor au responsabilitatea de a promova cunoștințe despre securitatea cibernetică printr-o comunicare eficientă și programe de formare continuă. Aceste inițiative ajută angajații să identifice și să răspundă adecvat la amenințările cibernetice. Simulările de incidente de securitate sunt, de asemenea, esențiale pentru a testa și a îmbunătăți constant răspunsurile la incidente.

Reglementările actuale obligă implicarea managementului organizației, managerilor de departament, managerilor de proiect și a tuturor angajaților alături de departamentul IT în procesul de asigurare a securității cibernetice al organizației.

Securitatea cibernetică se va impune ca un pilon fundamental în adoptarea și integrarea tehnologiilor emergente, cum ar fi inteligența artificială, blockchain, calculul cuantic și metavers. În acest context, este esențial ca managementul să plaseze securitatea cibernetică în centrul strategiilor decizionale, reflectând astfel importanța și complexitatea crescută a acestui domeniu în ultimul deceniu. Organizațiile trebuie să inițieze și să dezvolte departamente specializate care să se ocupe exclusiv de securitatea specifică fiecărei noi tehnologii. Aceasta nu doar că va proteja resursele valoroase și va minimiza riscurile, dar va și asigura o tranziție sigură și eficientă către noile paradigme digitale. Astfel, securitatea cibernetică trebuie să devină o prioritate strategică imediată, integrată în toate nivelurile de planificare și executare la nivel corporativ.

CUM POATE FI RESPECTAT?

- **Formare Continuă:** Organizarea de sesiuni de formare periodice pentru a educa angajații despre noile amenințări cibernetice și practici de prevenire.
- **Politici de Securitate:** Crearea și implementarea unor politici de securitate cibernetică cunoscute și respectate de întregul personal, nu doar de echipa IT.
- **Sistem de Raportare:** Implementarea unui sistem deschis pentru raportarea incidentelor și vulnerabilităților de securitate, fără teama de represalii.
- **Evaluări de Securitate**: Integrarea evaluărilor de risc cibernetic în reviziile de business periodice pentru aliniere la strategia organizației.
- **Departament dedicat Cyber:** Înființarea unui departament Cyber, care să se ocupe de implementarea și supravegherea măsurilor de securitate cibernetică.

CE AR TREBUI SĂ ȘTIM?

1. Cine sunt atacatorii pentru business-ului meu?
2. Unde sunt vulnerabilitățile prioritare in business-ul meu?
3. Care este impactul unui incident cibernetic asupra business-ului? Unde este cel mai mare impact?
4. Ce apăr? Cum apăr businessul în caz de atac cibernetic?
5. Cu cine fac Planul de apărare?
6. Cum verific implementarea și evaluarea Planului?
7. Care este bugetul optim pentru realizare, implementare și monitorizarea Planului de apărare?
8. Cum informez / pregătesc angajații, partenerii și clienții pentru respectarea Planului de cyber security?

2. Implicarea managementului în identificarea și evaluarea riscurilor cibernetice la nivelul organizației

Reducerea potențialelor riscuri asociate securității cibernetice se realizează prin adoptarea de măsuri de verificare și control la toate nivelurile structurale ale unei organizații. Pentru o organizație, din punct de vedere managerial și operațional, asigurarea unui mediu securizat prin utilizarea sistemelor informatice reprezintă cerințe obligatorii, devenind practic o preocupare intensă și continuă în raport cu riscurile și amenințările posibile. Implicarea activă a managementului poate asigura o mai bună înțelegere a riscurilor cibernetice, o mai mare responsabilitate în implementarea măsurilor de securitate și o mai bună pregătire în fața potențialelor incidente de securitate.

În domeniul securității cibernetice, capacitatea decizională și de asumare a răspunderii de către conducerea unei companii este esențială și necesită dezvoltarea unor abilități manageriale cum ar fi capacitatea de comunicare, organizare, control și coordonare.

Obiectivele securității cibernetice au devenit din ce în ce mai complexe, având ca principal scop protecția datelor și a informațiilor ca resurse critice ale companiei. Valoarea datelor și a informațiilor necesită administrarea riscurilor asociate, raportarea și evaluarea corespunzătoare, de la nivelul managerial până la cel de execuție, printr-o politică strâns corelată cu strategia și procesele de lucru, prin promovarea celor mai bune practici din domeniu.

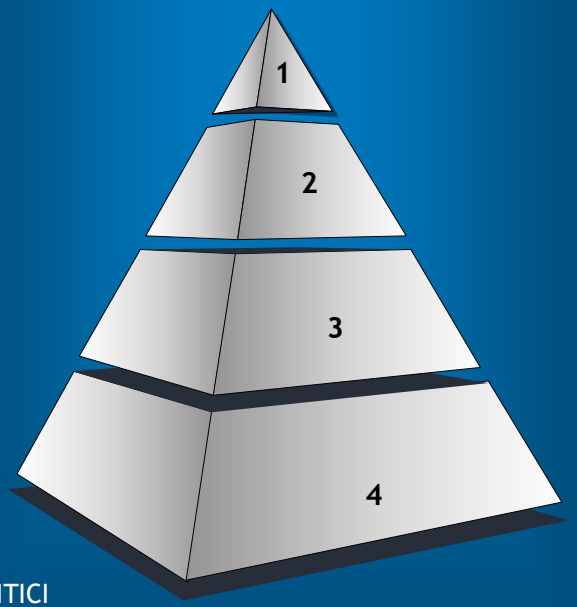
Minimizarea riscurilor (politici, proceduri, regulamente)

Fundamentul asigurării securității informației constă în dezvoltarea unor planuri, norme, politici de protecție și acțiune în cazul unor acțiuni care au ca scop compromiterea informațiilor și datelor. Asigurarea și dezvoltarea unui cadru general de concepere și aplicare a unor planuri, politici de securitate, modalități de evaluare și răspuns la incidente, monitorizare activă și/sau pasivă a sistemelor.

1. **Evaluare**: activități manageriale (politici de securitate, proceduri, reglementări, experiență post-incident) și acțiuni tehnice de inventariere a componentelor sistemului;
2. **Protecție**: dezvoltare și implementare a unor măsuri de prevenire și protecție pe baza estimărilor realizate în etapa de evaluare;
3. **Detecție**: identificarea incidentelor (intruziunilor), cu rol de a oferi suficient timp pentru a opri compromiterea (activități de colectare, monitorizare și audit);
4. **Răspuns la atacuri**: adoptarea măsurilor pentru restaurarea funcționalității și alegerea remediilor legale (validare, izolare sau eradicare incident, refacere sau investigații post-incident).

Sistemul de Management al Securității

Pentru a asigura protecția informațiilor, organizațiile trebuie să implementeze reguli și controale pentru date și informații, cât și pentru sistemele care stochează și procesează informațiile. Acest lucru se realizează prin dezvoltarea și aplicarea unor politici de securitate, standarde, norme și proceduri precum **Planul de securitate** (document care descrie modul în care organizația abordează și tratează



1. POLITICI
2. STANDARDE - cerințe specifice obligatorii
3. GHIDURI DE APLICARE - recomandări, bune practici
4. PROCEDURI - instrucțiuni pas cu pas

incidentele de securitate) și **Politica de securitate** (asigurarea protecției datelor și dezvoltarea unui mediu sigur de utilizare, care trebuie să se adapteze la obiectivele strategice și operaționale).

Procesul de management al riscurilor cibernetice

În contextul creșterii dependenței proceselor organizaționale de tehnologia informației, managementul riscurilor devine critic. Riscul, definit ca probabilitatea și impactul evenimentelor, se evaluează folosind instrumente precum matricea de evaluare a riscurilor.

Procesul include evaluarea riscurilor, coordonarea decizională, implementarea controalelor și măsurarea eficacității acestora. **Metodologiile de evaluare, precum ISO/IEC IS 13335-2, ISO/IEC IS 27005, MEHARI și NIST SP 800-30** orientează gestionarea riscurilor, oferind recomandări pentru tratarea și monitorizarea acestora. Analizele cantitative, calitative și cost-beneficiu sunt integrate în acest proces complex pentru a asigura o gestionare eficientă a riscurilor cibernetice.

Cybersecurity as a Service

Integrarea principiilor de securitate cibernetică este crucială în dezvoltarea și achiziția de tehnologie. Este esențial să asigurați lanțul de aprovizionare și să implementați politici eficiente de gestionare a riscurilor. Achizițiile trebuie să respecte principiile de securitate prin design, selectând furnizori care oferă soluții sigure și conforme.

Comportamentul și comunicarea la nivelul departamentelor din cadrul companiei (intern)

Promovați o cultură de securitate cibernetică printr-o comunicare onestă și transparentă în cadrul companiei. Încurajați colaborarea și feedbackul constructiv pentru a învăța și a îmbunătăți practicile de securitate. Utilizați instrumente adecvate pentru colectarea incidentelor și comunicarea eficientă între departamente, consolidând astfel securitatea organizațională. Încurajați educația în locul disciplinării/ mustrării în cazul unor greșeli făcute de angajați, pentru a încuraja reportarea imediată a incidentelor; punerea accentului pe mustrare poate duce la frica angajatului de a reporta, ceea se va dovedi contraproductiv pe termen lung.

Cooperare și colaborare cu autoritățile competente în domeniu la nivel național (extern)

- Raportează incidentele la autoritățile naționale competente! **Cum se raportează? Sunând la numărul unic de urgență pentru atacuri cibernetice 1911 sau trimițând un e-mail la alerts@dnsc.ro**.
- Încurajați implicarea în programe specializate de prevenire a incidentelor (Bug Bounty, Coordinated Vulnerability Disclosure etc).
- Este necesar ca organizația să aibă Implementat un plan de comunicare (ghiduri, proceduri) pentru colaborarea cu autoritățile cu atribuții in domeniu.

CUM POATE FI RESPECTAT?

- Încurajarea colaborării între departamente, resursele tehnice, lanțul de aprovizionare și clienți pentru alinierea măsurilor de securitate cu obiectivele de business și strategiile de gestionare a riscurilor.
- Susținerea evaluărilor și a auditului periodic privind riscul organizațional pentru a identifica vulnerabilitățile din punct de vedere al securității cibernetice.
- Colaborarea cu experți și entități externe, specializate în securitate cibernetică pentru evaluări și îndrumări independente adaptate companiei dvs.
- Creșterea gradului de conștientizare a tacticilor de inginerie socială și facilitarea unei culturi care încurajează raportarea incidentelor.
- Încurajarea investițiilor în capabilitățile de apărare cibernetică pentru companie.
- Adoptarea de măsuri preventive, ale căror costuri trebuie echilibrate cu potențialele daune cauzate de exploatarea vulnerabilităților.

CE AR TREBUI SĂ ȘTIM?

1. Care este rolul managementului în evaluarea și gestionarea riscului cibernetic în cadrul organizației?
2. Există definite măsuri de control care implică politici, procese, proceduri care sunt implementate, monitorizate, revizuite și îmbunătățite?
3. Există la nivelul organizației definit un Sistem de Management al Securității (ISMS)?
4. Există la nivelul companiei definit un cadru organizațional privind managementul riscurilor cibernetice?
5. Există la nivelul companiei cunoștințe privind metode si tehnici de identificarea și evaluarea riscurilor?
6. Există la nivelul companiei o abordare metodologică privind managementul riscurilor cibernetice?

3. Implicarea activă a managementului în tratarea și monitorizarea riscurilor cibernetice

Implicarea managementului în procesul de tratare și monitorizare a riscurilor cibernetice este un pas esențial pentru asigurarea securității informaționale a unei organizații. Managementul trebuie să fie profund conștient de riscurile cibernetice actuale și potențiale, să prioritizeze și să aloce resurse adecvate pentru prevenirea și combaterea acestora.

Tratarea riscurilor este un proces fundamental în gestionarea riscurilor, fie ele legate de securitatea cibernetică sau de alte domenii. Există patru strategii principale de tratare a riscurilor: acceptarea, diminuarea, evitarea și transferul riscului.

- **Acceptarea riscului** - Această strategie implică recunoașterea și acceptarea faptului că riscul există și că poate avea consecințe negative. Organizațiile decid să accepte riscul atunci când costurile implementării unor măsuri de gestionare a riscurilor sunt mai mari decât beneficiile obținute. Este important de menționat că acceptarea riscului nu înseamnă ignorarea acestuia, ci este o alegere conștientă bazată pe o evaluare a costurilor și beneficiilor.
- **Diminuarea riscului** - Această strategie implică adoptarea de măsuri pentru a reduce probabilitatea sau impactul riscului. Acest lucru poate include implementarea de controale de securitate, îmbunătățirea proceselor operaționale, actualizarea sistemelor și a software-ului, educarea angajaților în domeniul securității cibernetice etc. Scopul este de a reduce riscul la un nivel acceptabil și de a minimiza eventualele daune în cazul în care riscul se materializează.
- **Evitarea riscului** - Această strategie implică luarea de măsuri pentru a elimina sau a evita complet riscul. Organizațiile pot alege să evite riscul prin renunțarea la anumite activități sau practici care ar putea expune la riscuri. De exemplu, o companie ar putea evita riscul de a fi afectată de un atac cibernetic prin renunțarea la utilizarea anumitor tehnologii sau sisteme considerate prea vulnerabile.
- **Transferul riscului** - Această strategie implică transferul parțial sau total al responsabilității și impactului riscului către o altă entitate, de obicei printr-o asigurare sau un acord contractual. De exemplu, o organizație poate transfera riscul cibernetic prin achiziționarea unei polițe de asigurare cibernetică, care acoperă daunele financiare în cazul unui incident de securitate cibernetică.

Monitorizarea periodică a riscurilor cibernetice este un proces continuu, iar amenințările pot apărea sau evolua rapid. Monitorizați-vă riscurile pentru a vă asigura că sunt încă acceptabile, revizuiți controalele pentru a vă asigura că sunt încă adecvate scopului pentru care au fost implementate și faceți modificările necesare unde este cazul. Riscurile se schimbă continuu pe măsură ce peisajul amenințărilor cibernetice evoluează, iar sistemele și activitățile în cadrul organizației se schimbă.

Această monitorizare ar trebui să includă o analiză a incidentelor de securitate anterioare pentru a identifica tendințe care ar putea indica riscuri sau vulnerabilități existente sau emergente în infrastructura sau procesele organizației. Această analiză poate oferi informații valoroase pentru îmbunătățirea strategiilor de gestionare a riscurilor și pentru prevenirea incidentelor viitoare.

CUM POATE FI RESPECTAT?

- Implementarea unei strategii de tratare a riscurilor poate necesita investiții financiare semnificative pentru achiziționarea de tehnologii, software și alte instrumente de securitate cibernetică, precum și pentru formarea și instruirea personalului. Aceste costuri pot include și achiziționarea de asigurări cibernetice pentru transferul riscurilor și pentru acoperirea eventualelor daune financiare.
- Monitorizarea riscurilor cibernetice necesită o serie de resurse, inclusiv tehnologie, personal specializat și procese bine definite, programe de formare și educație continuă pentru angajați si planuri de rezervă și de continuitate a afacerii.

CE AR TREBUI SĂ ȘTIM?

1. Cum se decide răspunsul la risc?
2. Cum monitorizăm și gestionăm vulnerabilitățile în infrastructura noastră IT?
3. Cum ne asigurăm că personalul nostru este pregătit să reacționeze la incidente cibernetice?

4.Securitatea cibernetică previne pierderile financiare semnificative

Neglijarea amenințărilor și riscurilor aferente securității cibernetice a organizației poate avea consecințe financiare semnificative. În prezent, securitatea activelor și proceselor digitale este la fel de importantă precum cea a activelor și proceselor fizice.

Există o concepție eronată conform căreia numai marile corporații sunt expuse atacurilor cibernetice. În realitate, fiecare organizație - de la startup-uri până la companii mari, operând în diverse industrii - se confruntă cu amenințări cibernetice care nu țin cont de domeniul sau de dimensiune afacerii.

Deși sentimentul general și atenția acordată securității cibernetice sunt în creștere, persistă o discrepanță notabilă între liderii de organizații cu privire la urgența și semnificația securității cibernetice. Acest fapt nu doar că reflectă o neînțelegere a dimensiunii potențialelor riscuri, dar și o subestimare a impactului pe care un atac cibernetic îl poate avea asupra continuității afacerii.

În ultimul deceniu, domenii de activitate odată considerate imune la riscurile digitale au devenit progresiv mai vulnerabile în fața amenințărilor cibernetice. Evoluția actuală a dinamicii concurențiale pe piață impune adoptarea soluțiilor digitale care, deși generează avantaje semnificative din punct de vedere operațional și financiar, deschid simultan noi dimensiuni pentru atacurile cibernetice.

Conștientizarea faptului că fiecare întreprindere, indiferent de activitatea sa principală, se află pe câmpul de luptă digital devine tot mai necesară. Însă, adesea este necesar un impact direct - un atac cibernetic - pentru a trece de la complacere la acțiune. Securitatea cibernetică sporită a companiei nu înseamnă întotdeauna creșterea bugetelor, cheltuielilor sau a numărului de angajați, ci mai mult un mod cât mai larg de a gândi businessul interconectat cu responsabilități, investiții, efort distribuit și o atitudine de cooperare cu angajații, clienții, partenerii și instituțiile guvernamentale.

După numeroase incidente, ar trebui să fie evident că securitatea cibernetică este un aspect crucial pentru companii din toate domeniile, de la cele care oferă servicii directe digitale, precum centrele de date, producătorii de hardware[3] și furnizorii de internet, până la acelea care "vând rotopercutoare"[4], administrează porturi[5] sau operează în sectorul farmaceutic. În lipsa unor măsuri proactive, companiile se expun riscului de a suferi pierderi atât de semnificative, ce pot duce la faliment.

Managementul organizației trebuie să înțeleagă faptul că securitatea cibernetică nu este o opțiune, ci o necesitate absolută, la fel de critică pentru supraviețuirea și prosperitatea afacerii ca și securitatea fizică a activelor sale. Reflectând asupra diversității industriilor și rolului central al tehnologiei în operațiunile zilnice, devine esențial să înțelegem cum specificul fiecărei industrii o face vulnerabilă la riscuri cibernetice particulare.

[3] Ace Hardware Still Reeling from Weeklong Cyberattack (darkreading.com)

[4] The Home Depot reportedly ignored warnings from its own cybersecurity team - The Verge

[5] DP World says hackers stole Australian ports employee data | Reuters

CUM POATE FI RESPECTAT?

- Cursuri de formare în securitatea informației, disponibile online și offline.
- Consultanță și audituri de securitate cibernetică oferite de firme specializate.
- Ghiduri publicate de instituții naționale și internaționale de securitate cibernetică.

CE AR TREBUI SĂ ȘTIM?

1. Ce date sensibile deține compania noastră și unde sunt stocate?
2. Care este apetitul de risc cyber al companiei din punct de vedere financiar?
3. Planul de răspuns la incidente include evaluarea rapidă a impactului financiar?
4. Ce resurse sunt considerate ținte prioritare în scenariile de atacuri cibernetice?
5. Ce măsuri proactive sunt puse în practică pentru a reduce impactul financiar al unui atac?

5.Conducerea are datoria de a promova specializarea angajaților

Este crucial ca managementul organizațiilor să pună accent pe specializarea angajaților în domeniul securității cibernetice, subliniind importanța cunoștințelor și competențelor specifice. Acest lucru poate fi realizat prin dezvoltarea de competențe cyber la nivelul departamentului IT, prin dezvoltarea unei echipe dedicate pentru securitate cibernetică sau prin colaborarea cu specialiști externi, pentru a asigura o apărare eficientă împotriva amenințărilor și pentru a întări reziliența organizației în fața atacurilor cibernetice. Implementarea unei strategii de specializare nu doar că va întări reziliența organizației în fața amenințărilor, dar va și contribui la crearea unei culturi de securitate care valorizează cunoașterea, competența și inovația în acest domeniu.

Ideal, ar trebui sa existe și un departament de securitatea cibernetică independent de IT, pentru a evita conflictele de interese și pentru a asigura o concentrare specializată. Profesioniștii IT sunt responsabili cu menținerea și securizarea infrastructurii tehnice, incluzând servere, rețele și alte dispozitive. Personalul de securitate cibernetică prioritizează aspectele de securitate, implementând măsuri tehnice și răspunzând la amenințări. În contexte cu resurse limitate, combinarea rolurilor creează provocări, deoarece responsabilitățile duble pot intra în conflict, departamentul IT prioritizând funcționalitatea.

Chiar dacă sistemele de securitate cibernetică devin tot mai sofisticate, factorul uman rămâne principala slăbiciune în fața atacurilor cibernetice. O eroare din partea unui angajat nespecializat, lipsa de conștientizare a riscurilor sau o simplă neglijența pot oferi o cale de acces facilă pentru hackeri.

Un exemplu elocvent este breșa de securitate de la Equifax[6] din 2017, care a expus datele personale a 148 de milioane de americani. Atacul a fost posibil din cauza lipsei de pregătire a personalului responsabil de securitatea cibernetică. Deși Equifax a externalizat anumite componente cyber, lipsa de control și monitorizare a permis atacatorilor să obțină acces neautorizat la sistemele interne.

Un alt exemplu semnificativ este atacul WannaCry[7], care a vizat peste 200.000 de dispozitive din 150 de țări. Succesul său s-a datorat lipsei de actualizare a sistemelor Windows, separării insuficiente a rețelelor interne și a copiilor de siguranță deficitare din partea multor companii. Impactul unor astfel de incidente poate fi drastic diminuat sau chiar eliminat prin specializarea continuă a personalului.

Managementul organizației joacă un rol major în asigurarea competențelor necesare echipei de securitate cibernetică. Este necesar ca aceștia să recunoască importanța investițiilor în formarea angajaților, creând un mediu în care învățarea și actualizarea constantă a cunoștințelor sunt valori fundamentale. Aceasta implică nu doar furnizarea de resurse pentru obținerea de certificări profesionale recunoscute la nivel internațional, ci și promovarea unei culturi organizaționale care încurajează împărtășirea cunoștințelor și colaborarea.

CUM POATE FI RESPECTAT?

- Dezvoltarea internă de aptitudini cyber
- Stabilirea unui plan de dezvoltare profesională și certificare pentru echipa de securitate cibernetică;
- Evaluarea periodică a competențelor și a nevoilor de formare;
- Sprijinirea financiară a angajaților pentru a urma cursuri specializate și a obține certificate recunoscute la nivel internațional, ex: CompTIA Security+, CompTIA Network+ sau CISSP;
- Externalizarea serviciilor către specialiști în domeniu.

★

CE AR TREBUI SĂ ȘTIM?

1. Dispuneți de o echipă internă dedicată securității cibernetice?
2. Angajații din echipa de securitate cibernetică au experiență în domeniu și dețin certificări profesionale recunoscute?
3. Există un plan de dezvoltare profesională pentru echipa de securitate cibernetică și IT?
4. Investiți suficient în resurse și instrumente de securitate cibernetică?
5. Contractele cu furnizorii din lanțul de aprovizionare acoperă toate aspectele legate de securitatea informațională?

[6] Equifax data breach FAQ: What happened, who was affected, what was the impact? | CSO Online

[7] What was the WannaCry ransomware attack? | Cloudflare

6. Managementul organizațiilor trebuie să asigure conformitatea cu cerințele legale

Conformitatea cu cerințele legale aplicabile unei organizații presupune implementarea cerințelor legale în cadrul organizației prin politici, proceduri, decizii de management și procese interne.

Respectarea legilor reduce materializarea riscurilor, inclusiv prin incidente de securitate în domeniul securității cibernetice; legislația se concentrează, pe de o parte, pe măsuri organizatorice, inclusiv existența proceselor interne de gestionare a riscului. Aceste tipuri de măsuri asigură o creștere a capabilității organizației de a preveni, detecta și răspunde la incidente de securitate.

Pe de altă parte, legislația se concentrează și pe măsuri tehnice de prevenție și detecție a incidentelor de securitate. Acestea completează partea organizațională și necesită, de asemenea, aprobarea din partea managementului pentru implementare luând în considerare analiza de risc și apetitul la risc.

Ce rol are managementul în respectarea conformității? Managementul solicită și monitorizează identificarea legislației aplicabile organizației, verificarea conformității cu legislația identificată, precum și monitorizarea periodică a nivelului de conformitate, fiind responsabil pentru conformitatea cu legislația aplicabilă.

Managementul trebuie să fie activ implicat în luarea deciziilor privind modul de implementare a măsurilor interne organizaționale sau tehnice aferente conformității, precum și în aprobarea bugetului necesar pentru acestea.

Conformitatea nu înseamnă doar proceduri, ci și procese. Pentru a realiza conformitatea cu o cerință legală în domeniul securității cibernetice sunt necesare anumite măsuri tehnice (inclusiv soluții de securitate), însă sunt necesare anumite procese interne în cadrul organizației, cum ar fi procesul de gestionare a riscului. Acestea presupun și stabilirea de roluri și responsabilități în cadrul organizației, atât la nivel de management, cât și la nivel de departamente diferite, de la IT până la juridic, HR și vânzări.

Conformitatea include și ecosistemul de furnizori, iar pentru a respecta anumite cerințe legale, organizația trebuie să implice furnizorii săi. Acest lucru se realizează, în general, prin obligații specifice legate de securitatea cibernetică, care sunt asumate de furnizori, inclusiv prin acorduri contractuale. Aceste obligații sunt implementate de furnizori și monitorizate de organizație, folosindu-se metode precum raportările periodice și indicatorii de performanță (KPI) și de risc.

Verificarea conformității este un proces ciclic întrucât pot fi adoptate cerințe legale noi sau modificate cerințele legale existente; respectarea continuă a politicilor/procedurilor interne, precum și a proceselor interne de obicei necesită și monitorizare pentru buna lor funcționare; în cazul modificărilor interne ale organizației (e.g. utilizarea de noi tehnologii, achiziționarea unei alte societăți) pot apărea cerințe legale noi de implementat sau pot necesita ajustarea procedurilor/proceselor interne existente.

CUM POATE FI RESPECTAT?

- Solicită raportări privind statusul implementării legislației aplicabile, atât cea în vigoare, cât și monitorizarea legislației în curs de adoptare.
- Asigură existența de roluri și responsabilități, precum și procese interne corespunzătoare pentru implementarea și continuitatea respectării legislației aplicabile
- Solicită raportarea statusului pentru implementarea corespunzătoare a măsurilor tehnice, soluțiile de securitate și măsurile organizaționale pentru detecție, protecție, prevenție, remediere și recuperare.

CE AR TREBUI SĂ ȘTIM?

1. Ce legi sunt aplicabile organizației mele?
2. Care sunt obligațiile legale de implementat?
3. Care sunt acțiunile interne prin care pot implementa cerințele legale?
4. Care sunt departamentele interne care ar trebui implicate în implementare?
5. Este necesară implicarea unui consultant extern în implementare?
6. Cât de frecvent să raportăm statusul implementării cerințelor legale către management?
7. Care sunt rolurile si responsabilitățile din cadrul organizației pentru a asigura conformitatea cu legislația?
8. Cum putem monitoriza periodic conformitatea? Prin KPI, audit intern, audit extern?
9. Cine verifică periodic proiectele de legi pentru a identifica cerințe legale noi aplicabile organizației?
10. Cine verifică modificările din cadrul organizației pentru a identifica noi cerințe legale de implementat datorită acestor modificări?

REGLEMENTĂRI UE:

- Network and Information Security Directive (NIS 2)
- The Critical Entities Resilience (CER)
- Digital Operational Resilience Act (DORA)
- Cyber Security Act (CSA), Cyber Resilience Act (CRA)
- Cyber Solidarity Act, AI Resilience Act (ARA)
- Digital Services Act (DSA)
- Digital Markets Act (DMA)
- eIDAS Regulation

7.Continuitatea activității, managementul crizelor si reziliența cibernetică

Pentru organizații, la nivel global, cel mai important risc de business pentru anul 2024 este riscul incidentelor cibernetice, iar locul al doilea este ocupat de riscul de întrerupere a activității[8]; aceste două riscuri sunt pe primele două sau trei poziții în ultimii 9 (nouă) ani[9],[10]. În acest context, se recomandă ca managementul organizațiilor să aibă în vedere implementarea de măsuri, procese și sisteme care să asigure un grad înalt de reziliență organizațională și reziliență cibernetică.

Continuitatea activității se referă la capacitatea organizației de a continua să livreze produse sau servicii la nivele acceptabile și predefinite, în urma apariției unor incidente cu efect perturbator. Managementul Continuității Afacerii (BCM – Business Continuity Management) este un sistem de management prin care se planifică și se organizează continuarea activității pentru situația apariției unor incidente perturbatoare, inclusiv incidente cibernetice, și declanșarea unor scenarii care pot genera oprirea activității. Prin implementarea unui sistem de BCM, managementul organizației asigura procese și resurse necesare bunei gestionari a scenariilor de risc și a eventualelor crizelor generate de acestea, dar și restaurarea proceselor și reluarea activității într-un timp cât mai scurt, la costuri optime, precum si reducerea impactului, antrenarea managementului, a echipelor care gestionează crizele și a personalului implicat, la toate nivelurile.

Proiectul de implementare a Sistemului BCM, agreat și susținut de echipa de management, parcurge în general patru etape principale, conform framework-ului prezentat vizual în imaginea alăturată11. Planificarea restaurării proceselor se realizează prin intermediul unor planuri de continuitate a activităților, care este recomandat să fie revizuite și actualizate periodic, pentru asigurarea coerenței la nivelul organizației.

[8] Allianz Risk Barometer 2024

[9] International Conference on Business Excellence 2024

[10] Allianz Risk Barometer 2015-2024

[11] Rethink BCM & BC Consulting Group

CUM POATE FI RESPECTAT?

- Sistem de Management al Continuității Activității bazat pe management al riscurilor
- Digitalizarea proceselor de Management al Riscurilor, Management al Continuității Activității, Management al crizelor
- Resurse utile riscurilor
- Software dedicat pentru sistemul de management al continuității activității și management al crizelor

CE AR TREBUI SĂ ȘTIM?

1. Care este lista proceselor de business? Sunt acestea prioritizate prin analiza de impact?
2. Care sunt metodele de analiză a riscurilor și cum se pot identifica scenariile de risc cu potențial perturbator asupra continuității activității organizației?
3. Există planuri de continuitate a activității organizației?
4. Există back-up pentru datele și aplicațiile critice?
5. Există, în cadrul organizației, exerciții pentru simularea și testarea planurilor de continuitate, "table top exercises”?

Managementul crizei se definește, se organizează și se implementează cu acordul managementului, pentru fiecare tip de scenariu de risc relevant. Pentru riscurile cibernetice, structura echipei de management al crizei cibernetice la nivelul organizației este recomandat să cuprindă roluri atât la nivel de top management, cât și la nivel strategic și tactic, incluzând lideri și experți în IT și securitate cibernetică, dar și experți și personal operativ din cadrul funcțiunilor operaționale și de suport. Totodată, este recomandat să se creeze parteneriate cu experți în securitate cibernetică, respectiv companii externe, care să poată fi activate în cazul unor situații care impun expertiză de înaltă specializare în securitate cibernetică.

Sistemul BCM, odată implementat, devine un proces continuu al organizației și necesită angajamentul managementului, responsabilități atribuite în mod clar unor roluri din cadrul organizației sau crearea unor roluri și/ sau departamente dedicate, revizuire și actualizare regulată, alături de îmbunătățirea proceselor sale.

Reziliența cibernetică și reziliența organizațională sunt nu doar în responsabilitatea managementului, ci se bazează pe conștientizare, implicare si adaptabilitate la nivelul întregii organizații, iar o comunicare ș cooperare eficace și eficientă atât în plan orizontal cât și in plan vertical asigură bazele obținerii unor rezultate sustenabile. Analizele12 arată ca doar 27% din liderii de business au considerat că în 2023 organizația pe care o conduc este reziliență din punct de vedere cibernetic, în timp ce 29% din liderii cyber au considerat acest lucru, iar percepția asupra gradului de reziliență cibernetică este mai mare în rândul liderilor de business acolo unde aceștia au o comunicare regulată cu liderii din zona cyber.

Pentru creșterea rezilienței cibernetice și a celei organizaționale, se recomandă managementului organizațiilor să aplice strategii din sfera managementului continuității activității, cu tactici de implementare a unui Sistem de BCM. Studiile13 arată că 69% din organizații au înregistrat perturbări și/ sau întreruperi ale activității în ultimii doi ani, iar 91% dintre organizații au înregistrat cel puțin un astfel de eveniment perturbator, altul decât episodul pandemic generat de SARS-COV-2.

În contextul în care accesul la date este foarte important atât pentru echipele operaționale, echipele de specialiști, cât și pentru management în procesul decizional, cumulat cu modul de lucru hibrid sau în sistem de lucru la distanță extins la nivelul organizațiilor (în urma crizei generate de pandemia COVID-19), precum și cu agilitatea și adaptabilitatea necesare în situația riscurilor cibernetice, sistemul de BCM, alături de managementul riscurilor și gestionarea crizelor, pot fi implementate utilizând soluții software dedicate.

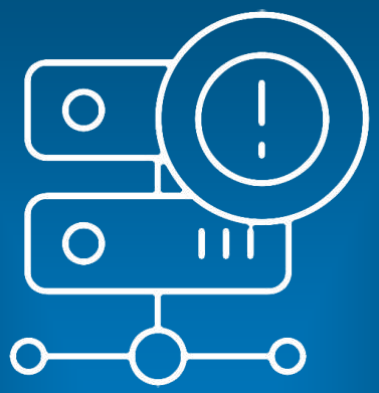
[12] Global Cybersecurity Outlook 2023

[13] Global Crisis and Resilience Survey 2023, PWC

Impactul și consecințele ignorării principiilor

Neglijarea principiilor de securitate cibernetică poate avea o serie de consecințe grave pentru o organizație, inclusiv:

1. **Pierderi materiale și de reputație** - acestea pot afecta grav credibilitatea organizației în fața clienților și în sectorul său de activitate, ducând la scăderea încrederii și potențiale pierderi de afaceri.
2. **Impact negativ asupra operațiunilor de business** - nerespectarea normelor de securitate poate perturba fluxurile operaționale, provocând întârzieri sau oprirea completă a activităților.
3. **Consecințe financiare** - riscurile securității cibernetice materializate pot genera costuri semnificative, de la daune directe cauzate de atacuri cibernetice, la pierderi de venituri și cheltuieli pentru recuperarea datelor.
4. **Creșterea vulnerabilităților** - neglijarea poate conduce la creșterea expunerii la noi atacuri cibernetice sau la alte evenimente neprevăzute care pot compromite securitatea organizației.
5. **Întreruperea fluxului de activitate** - atacurile cibernetice pot bloca sau perturba semnificativ operațiunile curente ale organizației.
6. **Cheltuieli suplimentare pentru remedierea daunelor** - acestea includ costuri pentru recuperarea după atacuri și pentru repararea prejudiciilor cauzate.
7. **Pierderea partenerilor și angajaților** - reputația afectată poate duce la pierderea încrederii din partea partenerilor de afaceri și a angajaților, afectând stabilitatea organizației.
8. **Furtul de date** - compromiterea datelor sensibile, inclusiv informații proprietare și personale, poate avea efecte devastatoare asupra securității și integrității organizației.
9. **Pierderea încrederii din partea clienților** - o breșă de securitate importantă poate eroda încrederea clienților și poate avea un impact negativ pe termen lung asupra reputației organizației.
10. **Sancțiuni legale** - nerespectarea legislației în vigoare poate atrage amenzi substanțiale sau alte tipuri de sancțiuni, inclusiv posibilitatea restricționării activităților.
11. **Costuri legate de conformitate** - după un incident, organizația poate fi nevoită să suporte costuri suplimentare pentru investigații, audituri și pentru a se conforma cerințelor legale, inclusiv cheltuieli juridice. De asemenea, se riscă amenzi costisitoare în urma legislațiilor europene (e.g. GDPR).



Concluzie

Securitatea cibernetică este crucială pentru sustenabilitatea și creșterea oricărei organizații în era digitală. Această responsabilitate nu revine doar departamentului IT, ci se extinde la întreaga structură managerială și la toate departamentele organizației. Prin urmare, este vital ca managementul să integreze securitatea cibernetică în strategia globală a companiei, să depășească granițele tehnice și să trateze aceste riscuri ca pe o prioritate strategică.

Este important ca fiecare membru al echipei de management să înțeleagă și să contribuie la implementarea practicilor de securitate cibernetică, subliniind necesitatea unei abordări multidisciplinare care să implice toate departamentele. Dezvoltarea unei culturi organizaționale care promovează și valorizează securitatea informațională este cheia pentru protejarea datelor și activelor companiei. În plus, conformitatea cu reglementările naționale și europene stricte, cum ar fi NIS 2, CER, DORA și alte acte normative, este vitală pentru asigurarea unui cadru de securitate robust și pentru minimizarea perturbărilor economice și sociale.

Prin urmare, acest ghid este destinat să servească ca un instrument pentru management, oferindu-le liderilor informațiile necesare pentru a înțelege și a gestiona eficient riscurile cibernetice. Așadar, este esențial ca managementul să aibă în vedere recomandările prezentate, să se angajeze în formarea continuă și să implementeze o strategie de securitate cibernetică integrată, care să protejeze organizația în fața amenințărilor în continuă evoluție.

În domeniul securității cibernetice, capacitatea decizională și de asumare a răspunderii de către conducerea unei organizații este decisivă și necesită dezvoltarea unor abilități manageriale cum ar fi comunicarea eficientă, capacitatea de conducere și organizare, capacitatea de control și capacitatea de coordonare.

ACEST MATERIAL A FOST REALIZAT DE:

Experți DNSC:

- Fraga Țariuc
- Aurel Huștea
- Laurențiu Zăbavă
- Antonio Radu
- Daniel Abotezătoaei

Experți externi:

- Larisa Găbudeanu
- Irina Coiciu
- Diana Nițescu
- Costel Ciuchi
- Cristi Caramitru

RECOMANDARE

Securitatea cibernetică reprezintă un pilon esențial în arhitectura oricărei entități moderne și trebuie să fie integrată în strategia de dezvoltare a fiecărei organizații. Transformarea digitală deschide porțile către eficiență și inovație, dar, în același timp, expune la riscuri cibernetice diverse, care necesită o gestionare atentă și proactivă.

În această nouă eră digitală, securitatea cibernetică trebuie să fie mai mult decât o serie de protocoale tehnice. Aceasta trebuie să fie o parte integrantă a viziunii strategice a fiecărei organizații, iar acest ghid este conceput să ofere instrumentele necesare pentru a naviga acest peisaj complex și pentru a transforma securitatea cibernetică într-un avantaj competitiv.

Cele șapte principii de securitate cibernetică descrise în acest material detaliază responsabilitățile specifice fiecărui nivel din organizație și oferă resurse valoroase, metodologii de referință și unelte practice pentru implementare. De asemenea, sunt incluse întrebări fundamentale care vor ajuta la evaluarea stadiului actual de securitate cibernetică din cadrul organizației, precum și la formularea unei strategii eficace de prevenire și răspuns la incidente.

În calitate de consultant cu o experiență de peste 25 de ani în domeniul securității cibernetice, al definirii de strategii și politici, al managementului riscurilor, în audit și conformitate, cât și în calitate de Director al Directoratului Național de Securitate Cibernetică (DNSC), consider că protecția spațiului cibernetic este una dintre responsabilitățile noastre fundamentale. Adoptarea măsurilor recomandate în acest ghid va fortifica organizația pe care o conduceți împotriva amenințărilor cibernetice și va sprijini consolidarea influenței dumneavoastră într-un mediu global interconectat. Recomand utilizarea acestui ghid pentru construirea unei strategii de securitate cibernetică robuste care va asigura că organizația dumneavoastră este bine pregătită să răspundă provocărilor de securitate cibernetică ale viitorului.

Dan Cîmpean

DAN CÎMPEAN

Directorul Directoratului Național de Securitate Cibernetică