Cyber MSME

Cybersecurity for Micro, Small & Medium Enterprises

Managementul crizelor: am fost atacat, ce fac acum?

De CTS Customized Training Solutions & CASE

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

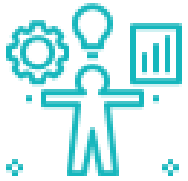
Obiective și scopuri

La finalul acestui modul, veți putea să:

- identificați crizele cibernetice din companie
- identificați potențialele riscuri
- evitați cele mai frecvente greșeli într-o criză
- îmbunătățiți sau creați un plan de gestionare a crizelor cibernetice
- vă pregătiți să soluționați criza cibernetică și să vă rederesați în urma acesteia

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Index



Unitatea 1: **Managementul crizelor cibernetice**

Unitatea 2: **Răspunsul pentru criza cibernetică**

Unitatea 3: **Recuperare după o criză cibernetică**

Unitatea 1: Managementul crizelor cibernetice

1.1: De ce aveți nevoie de un management al crizelor cibernetice?

Dacă gestionați un o firmă mică, probabil că nu aveți suficiente resurse și oameni pentru prevenirea și combaterea infracțiunilor cibernetice. Pentru întreprinderile mijlocii, este mai realist să delege câțiva specialiști care să lucreze la securitatea cibernetică. Cu toate acestea, chiar și cele mai mici afaceri ar trebui să se simtă obligate să îmbunătățească procedurile de gestionare ale crizelor cibernetice.

Protocoalele de management al crizelor cibernetice constau în 3 etape: 1) prevenire, 2) răspuns la criză și, în sfârșit, odată ce praful se așează 3) refacere. În acest modul, vă veți aprofunda cunoștințele referitoare la etapele 2 și 3.

Datorită acestui modul, vă veți îmbunătăți procedurile de gestionare a crizelor cibernetice, astfel încât să puteți face față atacurilor cibernetice.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 1: Managementul crizelor cibernetice

S1.2: Identificare crizei

În primul rând, trebuie să știți ce poate fi clasificat drept o criză cibernetică.

O criză cibernetică este orice eveniment cibernetic care poate să vă influențeze afacerea în mod negativ.

Exemple:

- dispozitive piratate
- screen mirroring pentru dispozitivele dvs
- e-mailuri copiate
- datele cardului de credit furate
- baza de date de clienți furată
- site-uri web distruse
- rețelele distruse
- refuzuri de serviciu etc.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 1: Managementul crizelor cibernetic

1.2: Identificarea crizei

Toate evenimentele cibernetice suspecte ar trebui să înceapă protocolul de criză cibernetică și să lanseze etapa 2 – răspunsul. Chiar dacă nu sunteți 100% sigur de ce s-a întâmplat, este mai bine să inițiați o acțiune. Amintiți-vă că o criză nu se referă numai la dvs. și la situația actuală a afacerii dvs. Următoarele aspecte sunt, de asemenea, importante:

- siguranța clienților și a partenerilor de afaceri
- profitabilitatea afacerii
- reputația ulterioară a afacerii

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Răspunsul la criza cibernetică

2.1: Rolul timpului

Reacția dvs la criza cibernetică trebuie să fie rapidă. Uneori aveți doar câteva secunde să faceți ceva, iar cel mai rău scenariu este să declanșați panica. Țineți minte că panica și frica vă pot costa întreaga afacere.

Cele mai frecvente greșeli în crizele cibernetice în IMM-uri

- nicio persoană(e) desemnată(e) responsabilă(e) de răspunsul la criza cibernetică
- informațiile de contact ale furnizorilor nu vă sunt la îndemână
- nu există un protocol pentru crizele cibernetice

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Răspunsul la criza cibernetică

2.1: Rolul timpului

De ce aveți nevoie de o persoană responsabilă de criza cibernetică?

Răspuns la criza cibernetică este orice acțiune care vă poate ajuta să gestionați o criză și să oferiți o actualizare stakeholderilor.

Răspunsul la criză cibernetică este un plan pe care îl implementați în situația unui atac. Când cineva vă atacă, nu aveți timp să vă gândiți la ce trebuie făcut. Toată lumea trebuie să fie pregătită. De aceea, trebuie să aveți una sau mai multe persoane responsabile de răspunsul la criza cibernetică.

Ce credeți, persoana responsabilă de crizele cibernetice trebuie să aibă un background în domeniul IT?

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Răspunsul la criza cibernetică

2.1: Rolul timpului

Nu sunteți sigur dacă persoanele responsabile de răspunsul la criza cibernetică ar trebui să aibă experiență IT? Ei bine, vă putem spune că mediul IT nu este cel mai important factor. De ce? La început, să aruncăm o privire asupra responsabilităților persoanei responsabile de răspunsul în fața unei crize cibernetice.

Responsabilitățile persoanei responsabile de crizele cibernetice

- să știe planul de rezervă
- să monitorizeze toate activitățile în timpul unei crize
- să conducă strategie internă
- să implementeze protocolul de comunicare în cazul unei crize

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Răspunsul la criza cibernetică

2.1: Rolul timpului

Dacă persoana responsabilă cu răspunsul la criză cibernetică are experiență în IT, el/ea s-ar putea să înțeleagă mai bine toți pașii necesari. Cu toate acestea, fără abilitățile de conducere și de management care sunt cruciale aici, o persoană IT nu poate implementa răspunsul la criza cibernetică.

Dacă aveți o micro-companie, este evident că trebuie să vă pregătiți pentru această posibilitate. Puteți semna, de asemenea, un acord cu un expert cibernetic în care aveți încredere. Firmele mici sau mijlocii ar trebui să numească un lider pentru etapa de răspuns la criza cibernetică.

Este bine de reținut că răspunsul la criza cibernetică poate fi implementat de la distanță.

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Răspunsul la criza cibernetică

2.2: Plan de rezervă

În MMSE, planul de rezervă poate diferi în funcție de ramură, tip de afacere etc.

Cu toate acestea, ar trebui să luați în considerare următorii pași:

Cunoașteți-vă furnizorii

Păstrați toate informațiile de contact ale furnizorilor dvs. (Internet, cloud, găzduire etc.) într-un mod sigur, deconectat. Deoarece atacul poate fi efectuat din rețeaua locală, chiar dacă nu sunteți conectat la Internet, parolele și datele sensibile vă pot fi furate.

A face:

Luați în considerare toate atacurile posibile înainte de a avea loc. Păstrați toate contactele importante nu numai online, ci și în versiunea tipărită.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Răspunsul la criza cibernetică

2.2: Planul de rezervă

Analizați urmele

Dacă observați acțiuni suspecte:

- pe contul dvs. bancar, sunați banca și blocați toate cardurile de credit;
- în cloud-ul dvs. de afaceri, contactați furnizorul (prin telefon sau e-mail).

De făcut:

Evitați utilizarea aplicațiilorcare pot fi infectate. Contactați direct furnizorul.

scoateți ștecherul

Uneori, aceasta este singura modalitate de a opri atacul cibernetic.

De făcut:

Dacă observați evenimente suspecte pe computerul dvs. sau al angajatului dvs., scoateți ștecherul.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Răspunsul la criza cibernetică

2.3: Protocolul de comunicare în criza cibernetică

Gândindu-vă la răspunsul la o criză cibernetică, ar trebui să luați în considerare protocolul de comunicare în timp de criză. Aici cel mai important este întotdeauna timpul. Comunicați cât mai curând posibil cu stakeholderii și informați-i despre problemă. Dumneavoastră ar trebui să fiți sursa faptelor - nu ziarele sau rețelele sociale.

Arată-le stakeholderilor că vă pasă de ei și că ați luat deja măsurile adecvate pentru a minimiza consecințele crizei cibernetice.

Trebuie să fiți pregătit pentru acest pas înainte de atac, așa că pregătiți lista cu stakeholderi:

- clienți (mai ales dacă aveți o bază de date)
- parteneri de afaceri, sponsori și investitori
- furnizori
- vecini/alte afaceri din clădire (care ar fi putut fi atacați)

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Răspunsul la criza cibernetică

2.3: Protocolul de comunicare în criza cibernetică

De asemenea, trebuie să vă gândiți să faceți o declarație pe site-ul dvs. web/site-ul de socializare sau în alte surse media. Desigur, puteți delega unul dintre angajații dvs. pentru această sarcină.

Este esențial să vă actualizați în mod frecvent declarația. Părțile interesate și publicul dvs. trebuie să fie siguri că aveți grijă de datele lor. Amintiți-vă că rezultatul atacului cibernetic poate fi viitorul afacerii dvs.

Cum vorbiți despre o criză cibernetică?

- ✓ Vorbiți întotdeauna clar.
- ✓ Folosiți fapte, nu opinii.
- ✗ Evitați reacțiile emoționale.
- ✓ Dați răspunsuri directe la întrebări.
- ✗ Nu acuzați pe nimeni și nu cereți scuze până nu știți ce se întâmplă.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Răspunsul la criza cibernetică

3.1: Cum vă întoarceți la normal după o criză cibernetică?

După criza cibernetică, fiecare afacere trebuie să facă câțiva pași pentru a reveni la funcționarea normală.

Așa ajungem la a treia etapă a managementului crizelor cibernetice numită recuperare în caz de dezastru.

Recuperarea după criza cibernetică este procesul care ajută afacerile pentru a reveni la operațiunile normale.

Recuperarea după criza cibernetică include pași precum:

- evaluări (ale pagubelor, cauzelor, si managementul)
- lecții învățate
- îmbunătățiri planificate

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Răspunsul la criza cibernetică

3.2: Faceți evaluarea

Recuperarea începe după criza cibernetică. Pentru a vă asigura că afacerea va fi „vindecată” trebuie să faceți câțiva pași radicali. În primul rând, trebuie să găsiți aspectele care au favorizat atacul.

- Planificați întâlnirile de evaluare cu echipa dvs. pentru a discuta toate daunele produse în timpul atacului cibernetic. Găsiți și înțelegeți cauzele. Dacă este necesar, solicitați sprijin experților externi.

- Evaluați planul de management cibernetic. Discutați-l pas cu pas, toate acțiunile întreprinse, pentru a înțelege ce a mers prost.

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Răspunsul la criza cibernetică

3.3: Lecția învățată

În timpul sau după evaluare, creați o listă de vulnerabilități care au favorizat atacul cibernetic. Nu o luați personal. Nu vă gândiți la asta ca la un eșec. Mai important este să învățați din acest atac.

Dacă sunteți lider/ proprietar de afaceri, atitudinea dumneavoastră are un impact asupra angajaților dumneavoastră și părților interesate. Dacă considerați atacul ca un eșec sau acuzați în mod greșit unul dintre angajații dvs. ca fiind responsabil pentru acesta, acest lucru poate afecta viitorul afacerii dvs.

Rețineți că fiecare mișcare și acțiune pe care o faceți influențează nu numai acest moment și acest atac cibernetic, dar și reputația și rentabilitatea dvs. viitoare.

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Răspunsul la criza cibernetică

3.4: Planificați îmbunătățirile

Ultimul pas este analizarea tuturor lacunelor folosind fapte și date. Dacă aflați că atacatorul v-a spart afacerea pentru că unul dintre angajații dvs. și-a neglijat datoria, este mai bine să evitați reacțiile emoționale. Există mai multe moduri de a acționa în această situație deoarece fiecare caz este diferit.

Cu siguranță, puteți depune eforturi pentru a crea obiective pe termen scurt și lung pentru a elimina golurile. Fiecare decalaj este un indicator verificat în incident. Fiecare obiectiv presupune prevenirea unor atacuri similare în viitor.

Recuperarea după atacul cibernetic trebuie să elimine sau să minimizeze cauzele atacului menționat. Dacă acest lucru nu se întâmplă, lecția nu va fi învățată.

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Răspunsul la criza cibernetică

3.5: Studiu de caz

Este posibil să fiți piratat, indiferent dacă dețineți o întreprindere mică sau mare. Deținerea unei companii mai mari nu vă face mai sigur sau mai bine pregătit pentru criză. Cel puțin nu întotdeauna. Aruncați o privire la studiile de caz de mai jos.

Marriott International

Atacul cibernetic

Cunoscutul lanț de hoteluri, Marriott International, a fost spart în ianuarie 2020, dar atacul a trecut neobservat de companie până la sfârșitul lunii februarie. Hackerii care au obținut acreditările de conectare a doi angajați Marriott puteau avea acces la detaliile oaspeților. Compania a început propria anchetă.

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Răspunsul la criza cibernetică

3.5: Studiu de caz

Răspuns

Marriott a făcut o declarație că hackerii ar putea obține detalii personale, cum ar fi nume, date de naștere, numere de telefon, preferințe de limbă și numere de cont de fidelitate. De asemenea, hotelul a trimis e-mail-uri oaspeților implicați; a creat un site web dedicat și un call center pentru a informa oaspeții. Marriott a asigurat că au asigurare, inclusiv asigurare cibernetică. Până acum totul pare profesionist, totuși, dând declarație compania nu credea că costurile sale totale legate de acest incident ar fi semnificative.

Recuperare

În octombrie 2020, organul de supraveghere al confidențialității datelor din Regatul Unit a amendat lanțul de hoteluri Marriott cu 18,4 milioane de lire sterline pentru o încălcare care ar fi putut afecta până la 339 de milioane de oaspeți.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Răspunsul la criza cibernetică

3.5: Studiu de caz

Unde a fost lecția învățată?

În primul rând, acesta nu a fost primul atac cibernetic asupra Marriott International. În 2014, hackerii au atacat grupul Starwood Hotels, care a fost achiziționat de Marriott doi ani mai târziu. După cum știm, compania nu a luat nicio măsură de recuperare la acel moment. De aceea următorul atac a fost mai ușor.

Primul atac observat public a avut loc în 2018. Din nou, protocolul de gestionare a crizelor nu a fost implementat corect, în consecință, până în acest moment atacatorul a continuat să aibă acces la toate sistemele afectate, inclusiv:

- nume
- adrese de email
- numere de telefon
- numerele de pașaport
- informații despre sosire și plecare
- Statut VIP
- numerele programului de loialitate

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Răspunsul la criza cibernetică

3.5: Studii de caz

Acesta este motivul pentru care Marriott a fost amendat de organul de control al confidențialității datelor din Marea Britanie. Lanțul hotelier nu a reușit să protejeze datele cu caracter personal, așa cum prevede Regulamentul general privind protecția datelor (GDPR). Mai mult, a eșuat de mai multe ori. Liderii responsabili cu managementul crizelor cibernetice nu au identificat și analizat lacunele în profunzime.

Ce a ajutat?

Marriott International oferă asigurări, inclusiv asigurări cibernetice. Acest lucru a ajutat la plata amenzilor.

Ce puteți învăța de aici?

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Răspunsul la criza cibernetică

3.5: Studii de caz

Lecții învățate:

- **Regândiți-vă la gestionarea crizelor cibernetice.**
- **Gândiți-vă dacă aveți suficiente abilități de conducere și management**

  implementați planul de gestionare a crizelor cibernetice
- **Dacă nu, aflați mai multe în celelalte cursuri ale noastre.**
- **De asemenea, căutați un expert cibernetic ca suport**
- **Gândiți-vă dacă aveți nevoie de asigurare cibernetică**

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unitatea 2: Răspunsul la criza cibernetică

3.6: Rezumat

În zilele noastre, managementul crizelor cibernetice este la fel de important entru o micro și o companie mare.

Diferența este în resursele pe care le aveți. Cea mai mică afacere are cele mai mari responsabilități.

Amintiți-vă că o criză cibernetică vă poate afecta compania chiar dacă nu este o afacere online tipică

(e-business). Ori de câte ori aveți nevoie de un laptop, smartphone, imprimantă, fax, cutie poștală, trebuie să luați în considerare

managementul securității cibernetice.

În cele din urmă, rețineți că o gestionare greșită poate escalada criza sau chiar poate crea una nouă.

Mult succes!

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Bibliografie și link-uri relevante

The New Statesman > **How to tell your customers you've been hacked**

https://www.newstatesman.com/spotlight/2019/09/how-tell-your-customers-you-ve-been-hacked

Deloitte > **Cyber crisis management: Readiness, response, and recovery**

https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-cm-cyber-pov.pdf

Security Boulevard > **Marriott Data Breach 2020: 5.2 Million Guest Records Were Stolen**

https://securityboulevard.com/2020/04/marriott-data-breach-2020-5-2-million-guest-records-were-stolen/#:~:text=The%2520breach%2520was%2520identified%2520at,have%2520accessed%2520the%2520guest%2520details.

BBC News > **Marriott Hotels fined £18.4m for data breach that hit millions**

https://www.bbc.com/news/technology-54748843

Marriott International News Center > **Marriott International Notifies Guests of Property System Incident**

https://news.marriott.com/news/2020/03/31/marriott-international-notifies-guests-of-property-system-incident

Forbes > **What Businesses Are The Most Vulnerable To Cyberattacks?**

https://www.forbes.com/sites/theyec/2021/01/19/what-businesses-are-the-most-vulnerable-to-cyberattacks/?sh=1c1c8f663534

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Mulțumim pentru atenție!

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.