AGENȚIA UNIUNII EUROPENE PENTRU SECURITATE CIBERNETICĂ

Ghid privind securitatea cibernetică pentru IMM-uri

12 PAȘI

PENTRU SECURIZAREA AFACERII

Criza provocată de COVID-19 a arătat cât de importante sunt internetul și calculatoarele în general pentru IMM-uri. Pentru ca afacerea să funcționeze bine în timpul pandemiei, multe IMM-uri au fost nevoite să ia măsuri de continuitate a activității, precum trecerea la servicii de tip cloud, îmbunătățirea serviciilor oferite pe internet, optimizarea site-urilor și asigurarea condițiilor necesare muncii de la distanță.

Broșura de față prezintă 12 pași practici, de nivel avansat, prin care IMM-urile își pot securiza mai bine sistemele și întreaga afacere. Publicația însoțește un raport ENISA mai detaliat, intitulat **„Securitate cibernetică pentru IMM-uri – Provocări și recomandări”**.

1 CREAȚI O CULTURĂ A SECURITĂȚII CIBERNETICE

ATRIBUIȚI ACEASTĂ RESPONSABILITATE UNUI CADRU DE CONDUCERE

O bună securitate cibernetică este un element-cheie pentru reușita oricărui IMM. Responsabilitatea acestor funcții critice ar trebui atribuită unei persoane din cadrul organizației care va asigura resursele corespunzătoare pentru securitatea cibernetică, precum timpul alocat de personal, achiziționarea de software, servicii și hardware pentru securitate cibernetică, instruirea personalului și elaborarea de politici eficace.

OBȚINEȚI IMPLICAREA ANGAJAȚILOR

Câștigați implicarea angajaților printr-o comunicare eficientă din partea conducerii pe tema securității cibernetice, prin sprijinirea deschisă de către conducere a inițiativelor în domeniu, prin instruirea corespunzătoare a angajaților și prin introducerea de reguli clare și specifice pentru angajați în politicile de securitate cibernetică.

PUBLICAȚI POLITICILE DE SECURITATE CIBERNETICĂ

În politicile de securitate cibernetică ar trebui trasate reguli clare și specifice pentru angajați, referitoare la conduita așteptată din partea lor atunci când utilizează echipamentele, serviciile și mediul TIC ale companiei. Politicile ar trebui să sublinieze și consecințele pe care le-ar putea suferi un angajat în cazul nerespectării lor. Ele trebuie revizuite și actualizate regulat.

REALIZAȚI AUDITURI DE SECURITATE CIBERNETICĂ

Ar trebui efectuate audituri regulate, de către persoane cu competențe, cunoștințe și experiență adecvate. Auditorii ar trebui să fie independenți, fie că sunt contractanți externi sau interni pentru IMM-uri, și să nu aibă legătură cu operațiunile IT derulate zilnic.

NU UITAȚI DE PROTECȚIA DATELOR

Conform Regulamentul general al UE privind protecția datelor[1], orice IMM care prelucrează sau stochează date cu caracter personal ale rezidenților UE/SEE trebuie să asigure controale de securitate adecvate pentru protecția datelor. În acest sens, trebuie asigurat și faptul că orice terț care lucrează în numele IMM-ului are instituite măsuri de securitate adecvate.

1 Regulamentul general privind protecția datelor https://ec.europa.eu/info/law/law-topic/data-protection_ro

2

ASIGURAȚI INSTRUIRE ADECVATĂ

Oferiți regulat angajaților instruire privind conștientizarea securității cibernetice, pentru a vă asigura că pot recunoaște și gestiona diversele amenințări cibernetice. Aceste sesiuni de instruire ar trebui să fie adaptate IMM-urilor și să se axeze pe situații din viața reală.

Asigurați instruire specializată în domeniu responsabililor cu gestionarea securității cibernetice din cadrul întreprinderii, pentru a vă asigura că dispun de aptitudinile și competențele necesare pentru a-și îndeplini atribuțiile.

3

ASIGURAȚI GESITONAREA EFICACE A TERȚILOR

Asigurați-vă că toți furnizorii, mai ales cei cu acces la date și/sau sisteme sensibile, sunt gestionați în mod activ și că aplică nivelurile de securitate convenite. Ar trebui încheiate acorduri contractuale pentru reglementarea modului în care furnizorii îndeplinesc cerințele de securitate respective.

4 ELABORAȚI UN PLAN DE RĂSPUNS LA INCIDENTE

Elaborați un plan formal de răspuns la incidente care să conțină instrucțiuni, roluri și responsabilități clare, pentru a vă asigura că toate incidentele de securitate cibernetică sunt soluționate prompt, profesional și corespunzător. Pentru a răspunde rapid amenințărilor de securitate, cercetați ce instrumente ar putea monitoriza și crea alerte atunci când au loc activități suspecte sau încălcări ale securității.

5 SECURIZAȚI ACCESUL LA SISTEME

Încurajați toate părțile implicate să folosească o frază de acces, o secvență de cel puțin trei cuvinte obișnuite aleatorii combinate într-o expresie care să îmbine excelent securitatea și ușurința memorării. Dacă optați pentru o parolă tipică:

- alegeți o parolă lungă, cu litere mici și mari, eventual cu numere și caractere speciale;
- evitați cuvintele evidente cum ar fi „parolă” și secvențele de litere sau cifre precum „abc” sau „123”;
- nu folosiți informații personale care pot fi găsite online.

Indiferent că folosiți fraze de acces sau parole,

- nu le reutilizați în alte locuri;
- nu le comunicați colegilor;
- activați autentificarea dublă;
- utilizați un manager de parole specific.

6

SECURIZAȚI DISPOZITIVELE

Menținerea securității dispozitivelor folosite de personal, fie că sunt computere, laptopuri, tablete sau telefoane inteligente, este un pas esențial într-un program de securitate cibernetică.

ASIGURAȚI PERMANENT CORECȚIILE ȘI ACTUALIZĂRILE SOFTWARE NECESARE

Soluția ideală este utilizarea unei platforme centralizate pentru gestionarea corecțiilor. Este foarte recomandat ca IMM-urile:

- să-și actualizeze regulat toate programele software;
- să activeze actualizarea automată ori de câte ori este posibil;
- să identifice software-ul și hardware-ul care necesită actualizare manuală;
- să nu omită dispozitivele mobile și IoT.

ANTIVIRUS

Ar trebui implementată o soluție antivirus gestionată la nivel central pe toate tipurile de dispozitive, menținută la zi pentru a-i asigura permanent eficacitatea. De asemenea, nu instalați programe software piratate, deoarece pot conține malware.

UTILIZAȚI INSTRUMENTE DE PROTECȚIE PENTRU E-MAIL ȘI WEB

Adoptați soluții de blocare a mesajelor spam, a e-mailurilor care conțin linkuri către site-uri rău intenționate sau cărora le sunt atașate fișiere periculoase, de exemplu cu viruși, și a mesajelor de tip phishing.

CRIPTARE

Protejați datele prin criptare. IMM-urile ar trebui să asigure criptarea datelor stocate pe dispozitive mobile precum laptopuri, telefoane inteligente și tablete. În cazul transferurilor de date prin rețele publice, cum sunt rețelele Wi-fi din hoteluri sau aeroporturi, asigurați criptarea datelor fie prin folosirea unei rețele virtuale private (VPN), fie prin accesarea site-urilor prin conexiuni securizate care utilizează protocolul SSL/TLS. Asigurați-vă că site-urile proprii utilizează tehnologie adecvată de criptare pentru a proteja datele clienților cât timp circulă pe internet.

IMPLEMENTAȚI GESTIONAREA DISPOZITIVELOR MOBILE

Atunci când facilitează munca la distanță, multe IMM-uri permit angajaților să-și folosească propriile laptopuri, tablete și/sau telefoane inteligente. Acest lucru poate crea o serie de probleme de securitate, având în vedere stocarea pe dispozitivele respective a unor date sensibile ale companiei. Un mod de a gestiona acest risc constă în utilizarea unei soluții de gestionare a dispozitivelor mobile (MDM), care oferă IMM-urilor posibilitatea:

- să controleze ce dispozitive au acces la sistemele și serviciile companiei;
- să se asigure că dispozitivul are instalat un software antivirus actualizat;
- să stabilească dacă dispozitivul este criptat;
- să confirme dacă dispozitivul are instalate cele mai recente corecții software;
- să se asigure că dispozitivul este protejat prin cod PIN și/sau parolă;
- să șteargă de la distanță orice date ale IMM-ului de pe dispozitiv în cazul în care proprietarul acestuia raportează pierderea sau furtul dispozitivului sau la încetarea raporturilor de muncă dintre proprietarul dispozitivului și IMM.

7 SECURIZAȚI-VĂ REȚEAUA

UTILIZAȚI FIREWALLURI

Firewallurile gestionează traficul care intră și iese din rețea și reprezintă un instrument vital în protejarea sistemelor unui IMM. Ele ar trebui utilizate pentru a proteja toate sistemele critice, în special pentru a proteja rețeaua IMM-ului de restul internetului.

VERIFICAȚI SOLUȚIILE DE ACCES LA DISTANȚĂ

IMM-urile ar trebui să-și verifice regulat toate instrumentele de acces la distanță pentru a se asigura că sunt securizate, în special:

- asigurându-se că toate programele software de acces la distanță sunt actualizate și au instalate cele mai recente corecții;
- restricționând accesul la distanță din zone geografice suspecte sau de la anumite adrese IP;
- limitând accesul la distanță al angajaților numai la sistemele și computerele necesare pentru activitatea lor;
- asigurând parole puternice pentru accesul la distanță și, dacă este posibil, activând autentificarea dublă;
- asigurându-se că este activă soluția de monitorizare și alertare pentru a semnala suspiciunile de atacuri sau activitățile neobișnuite suspecte.

8 ÎMBUNĂTĂȚIȚI SECURITATEA FIZICĂ

Ar trebui instituite măsuri de control fizic adecvat în locurile unde sunt păstrate informații importante. De exemplu, un laptop sau un telefon de serviciu nu ar trebui lăsat nesupravegheat pe bancheta din spate a mașinii. Ori de câte ori un utilizator pleacă de lângă computer, ar trebui să-l blocheze. Ca alternativă, se poate activa funcția de autoblocare pe orice dispozitiv utilizat în scop de serviciu. De asemenea, documentele sensibile tipărite nu ar trebui lăsate nesupravegheate și ar trebui păstrate la loc sigur când nu sunt folosite.

9 ASIGURAȚI COPII DE REZERVĂ

Pentru a putea recupera informațiile esențiale ar trebui păstrate copii de rezervă, acestea fiind un mod eficace de redresare în caz de dezastru, de exemplu după un atac ransomware. La păstrarea copiilor de rezervă ar trebui aplicate următoarele reguli:

- realizați copiile regulat și automat ori de câte ori este posibil;
- păstrați copiile de rezervă separat de mediul de producție al IMM-ului;
- asigurați criptarea copiilor, în special dacă vor fi mutate dintr-un loc în altul;
- testați capacitatea de a restaura regulat datele din copiile de rezervă. În mod ideal, ar trebui realizat periodic un test integral de restaurare completă.

10

APELAȚI LA SOLUȚII DE TIP CLOUD

Deși aduc multe avantaje, soluțiile de acest tip prezintă câteva riscuri specifice pe care IMM-urile ar trebui să le aibă în vedere înainte de a apela la un furnizor de servicii cloud. ENISA a publicat un „Ghid privind securitatea serviciilor cloud pentru IMM-uri”[2], pe care IMM-urile ar trebui să-l consulte atunci când fac trecerea la acest tip de servicii.

La alegerea unui furnizor de servicii cloud, IMM-urile ar trebui să se asigure că acesta nu încalcă vreo lege sau reglementare prin stocarea datelor, în special a celor cu caracter personal, în afara UE/SEE. De exemplu, RGPD al UE interzice stocarea sau transmiterea în afara UE/SEE a datelor cu caracter personal ale rezidenților din UE/SEE, cu excepția unor condiții foarte specifice.

2 https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

11 SECURIZAȚI SITE-URILE ONLINE

Este esențial ca IMM-urile să asigure configurarea și întreținerea securizată a site-urilor proprii și protejarea corespunzătoare a datelor cu caracter personal sau financiar, cum ar fi datele cardurilor de credit. Acest lucru va presupune efectuarea unor teste regulate de securitate a site-urilor respective pentru a identifica orice potențială vulnerabilitate, precum și efectuarea de verificări regulate pentru a asigura faptul că site-ul este întreținut și actualizat corespunzător.

12 CĂUTAȚI ȘI DISEMINAȚI INFORMAȚII

Un instrument eficace de combatere a criminalității cibernetice este diseminarea informațiilor. Diseminarea informațiilor referitoare la criminalitatea cibernetică este esențială pentru ca IMM-urile să înțeleagă mai bine riscurile cu care se confruntă. Atunci când firmele află despre problemele de securitate cibernetică și despre modurile în care au fost rezolvate de la firme similare, sunt șanse mai mari să ia măsuri pentru a-și securiza sistemele decât dacă ar afla astfel de detalii din rapoarte ale industriei sau din anchete privind securitatea cibernetică.

AGENȚIA UNIUNII EUROPENE PENTRU SECURITATE CIBERNETICĂ

DESPRE ENISA

Agenția Uniunii Europene pentru Securitate Cibernetică, ENISA, este agenția Uniunii dedicată realizării unui nivel comun ridicat de securitate cibernetică în întreaga Europă. Înființată în 2004 și consolidată prin Regulamentul UE privind securitatea cibernetică, Agenția Uniunii Europene pentru Securitate Cibernetică contribuie la politica cibernetică a UE, îmbunătățește fiabilitatea produselor, a serviciilor și a proceselor TIC prin sistemele de certificare a securității cibernetice, cooperează cu statele membre și cu organismele UE și ajută Europa să se pregătească pentru provocările cibernetice viitoare. Prin schimbul de cunoștințe, consolidarea capacităților și campanii de sensibilizare, agenția colaborează cu principalele părți interesate pentru a consolida încrederea în economia conectată, pentru a spori reziliența infrastructurii Uniunii și, ca scop final, pentru a menține securitatea digitală a societății europene și a cetățenilor. Pentru mai multe informații, consultați www.enisa.europa.eu.

ENISA

Agenția Uniunii Europene pentru Securitate Cibernetică

Biroul din Atena
Ethnikis Antistaseos 72 &
Agamemnonos 14,
Chalandri 15231, Attiki, Grecia

Biroul din Heraklion
95 Nikolaou Plastira
700 13 Vassilika Vouton
Heraklion, Grecia

enisa.europa.eu