Securitatea cibernetică și afacerea dumneavoastră

Costul criminalității cibernetice și cum să vă protejați datele

Oferit de

Cuprins

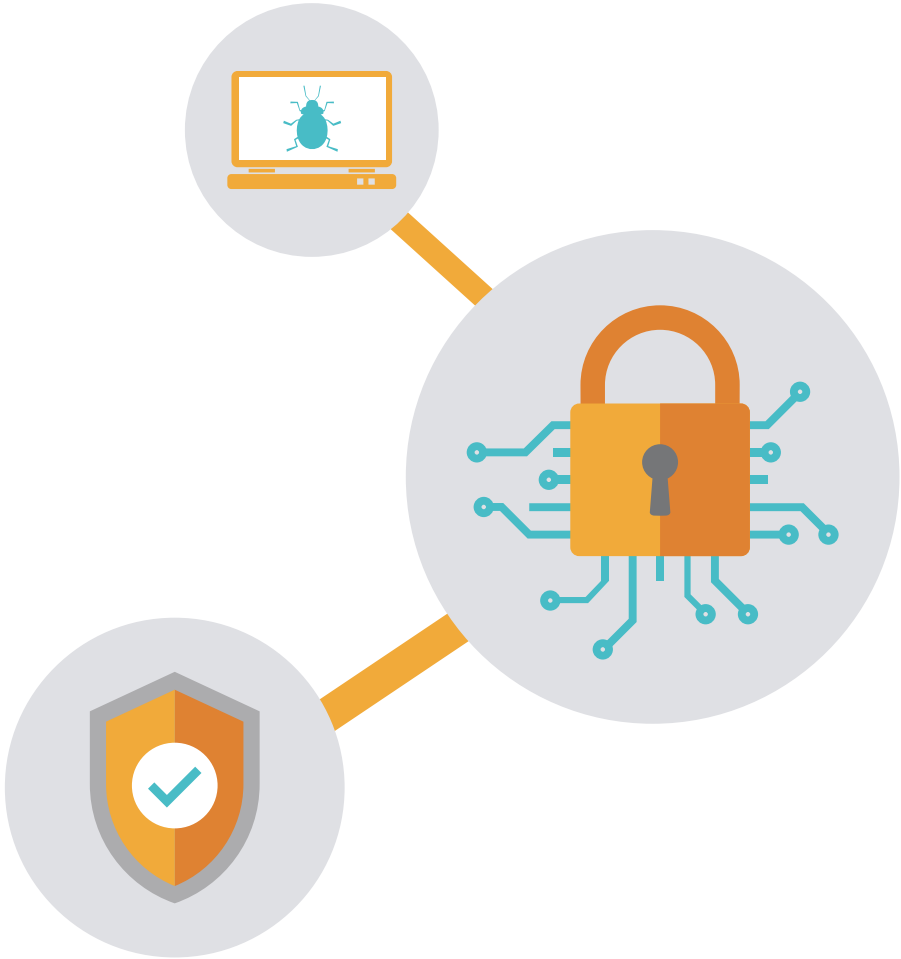
Introducere

„Mulți directori executivi declară că riscul cibernetic este riscul care va defini generația noastră”. – Dennis Chesley, consultant-șef la nivel global pe probleme de risc, PwC[1]

Securitatea cibernetică nu este o amenințare nouă. Însă este o amenințare în creștere. Hackerii sunt din ce în ce mai buni. Și au la dispoziție mai multe puncte prin care pot pătrunde într-o rețea. Internetul obiectelor multiplică numărul de dispozitive finale, care sunt adesea cea mai ușoară cale de pătrundere. Dimensiunea țintelor este în creștere, iar perturbările capătă o amploare din ce în ce mai mare.

În data de 21 octombrie 2016, furnizorul DNS din S.U.A. Dyn a suferit cel mai mare atac distribuit de tip DDoS (refuz serviciu) din istorie. Unele dintre cele mai mari site-uri web din lume - inclusiv Netflix, [2] Amazon și Twitter - au fost offline timp de mai multe ore.

În ianuarie 2017, Lloyds Bank a suferit întreruperi semnificative ale activității online. Clienții nu și-au putut verifica soldurile și nu au putut efectua plăți. Accesul din aplicațiile mobile a fost, de asemenea, întrerupt. Lloyds nu a confirmat nimic, însă s-a considerat că motivul cert a fost un atac DDoS.[3]



Surse: [1] PwC: Sondajul din 2016 privind starea globală a securității informațiilor [2] http://thehackernews.com/2016/10/dyn-dns-ddos.html [3] https://www.theguardian.com/business/2017/jan/23/lloyds-bank-accounts-targeted-cybercrime-attack

Introducere

Breșele de securitate similare înseamnă mai mult decât publicitate negativă. Ele implică cheltuieli importante.

În Raportul din 2016 elaborat pe baza sondajului despre securitatea imprimantelor, derulat de Spiceworks, 34% dintre organizații au afirmat că o breșă de securitate înseamnă mai mult timp petrecut cu apelurile/asistența oferită de birourile de resort, 29% au afirmat că breșele reduc productivitatea/eficiența, iar 26% au raportat un timp de nefuncționare sporit al sistemului, ca problemă majoră.[4]

Aproape 60% dintre responsabilii de securitate intervievați în cadrul unei evaluări IBM CSO au afirmat că nivelul de sofisticare al atacatorilor depășea nivelul de sofisticare al mecanismelor de apărare ale organizației lor.[5] Responsabilii de informații îngrijorați au afirmat timp de zece ani că securitatea cibernetică este una dintre cele mai importante 10 probleme, iar acum aceasta ocupă locul doi în studiul anual privind tendințele SIM.[6]

O mare parte din aceste pagube pot fi prevenite. În paginile următoare vom discuta despre idei greșite foarte răspândite referitoare securitatea cibernetică, vom analiza mai în detaliu impactul pe care criminalitatea cibernetică îl are asupra firmelor, precum și ce anume puteți face pentru a vă proteja mai bine împotriva atacurilor. În cele din urmă, vom privi către viitor și vom discuta despre ceea ce va urma și cum să ne pregătim în acest sens.

Surse: [4] Cercetarea derulată de HP privind securitatea imprimantelor în 2016, Spiceworks [5] Evaluarea IBM CSO din 2014 [6] Sondajul privind tendințele SIM ITdin 2015

Demontarea miturilor despre securitatea cibernetică

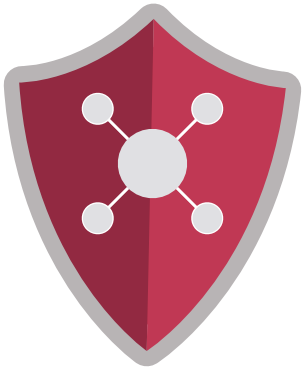
Cinci idei greșite foarte răspândite
care pot supune firmele riscului criminalității cibernetice

Gospodăriile se pot afla în fruntea breșelor de securitate în domeniul informațiilor, însă toate tipurile de organizații sunt supuse acestui risc. Iată cinci mituri despre securitatea cibernetică, care pot face ca firmele să devină vulnerabile în fața hackerilor.

Breșă de securitate

Scurgeri de informații securizate

Practici de securitate



Program antivirus

Atac cibernetic

1 Firmele își pot reveni rapid în urma unei breșe

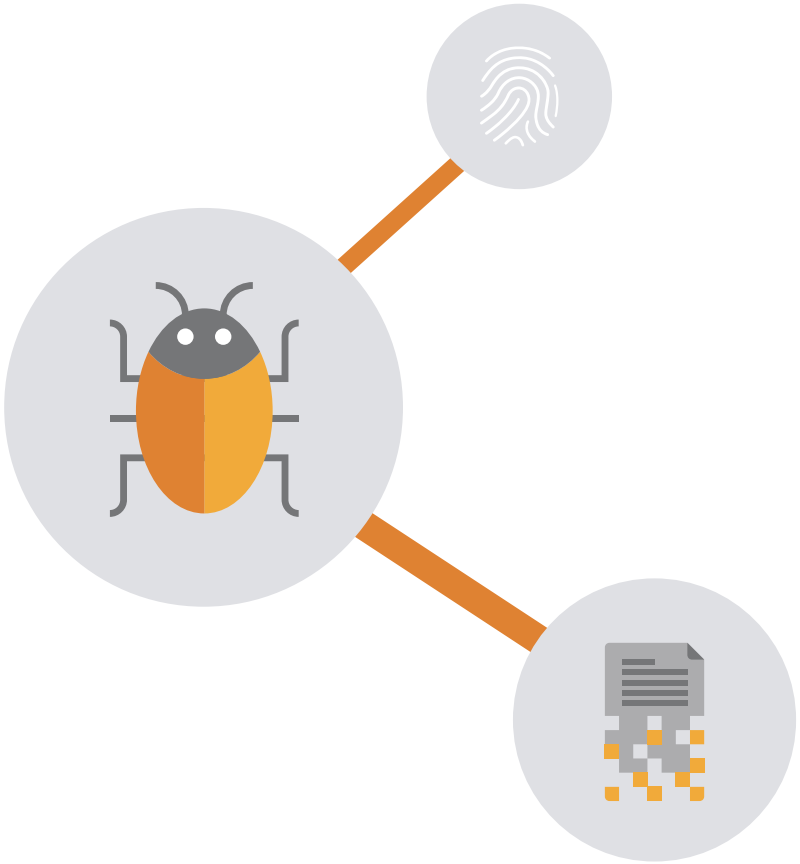
Totuși, este încă foarte dificil să se măsoare costul breșelor de securitate cibernetică pentru organizațiile comerciale. Opinia răspândită era aceea că se poate vedea impactul oricărei breșe prin scăderea prețului acțiunilor.

Însă prețurile acțiunilor sunt numai o componentă a situației, reprezentând doar începutul. În timp ce acțiunile își pot reveni în câteva săptămâni, costurile pe termen mai lung se acumulează. Noi programe de securitate. Înlocuirea personalului. Cheltuieli juridice.

Toți acești factori pot perturba în mod semnificativ activitatea pe perioade lungi de timp, după producerea unei breșe. Iar costurile cresc. Un studiu recent derulat de Ponemon a constatat că, pentru o breșă de securitate, costul mediu anualizat a crescut de la **7,7 milioane USD** în 2015 la **9,5 milioane USD** în 2016.[7]

Sursă: [7] Studiu derulat în 2016 de Institutul Ponemon privind costul criminalității cibernetice

2 Scurgerile de informații securizate se produc rareori, așadar nu este nevoie de o protecție deosebită



IDC a constatat[8] că proporția de firme care s-au confruntat cu o breșă de securitate a atins 99% în 2016. Iar numărul de firme care au raportat faptul că au fost victima intruziunilor cibernetice de 6-10 ori într-un an a crescut de la 9 procente în 2014 la 18,9 procente în 2016.[9]

Este posibil ca aceste cifre să fie subestimate. Breșele de securitate sunt adesea raportate în mod subestimat deoarece firmele încearcă să evite publicitatea negativă aferentă.

Celălalt aspect pe care acest mit nu îl ia în considerare este reprezentat de impactul debilitant pe care îl poate avea o breșă de securitate. Poate că societatea dvs. a fost victima doar a unei singure breșe de securitate. Însă chiar și o singură breșă ar putea genera probleme semnificative.

Surse: [8] IDC [9] Studiu derulat în 2016 de Institutul Ponemon privind costul criminalității cibernetice

3 Am angajat un specialist IT care să gestioneze aspectele legate de securitate, astfel încât nu mai este nevoie să știm alte lucruri

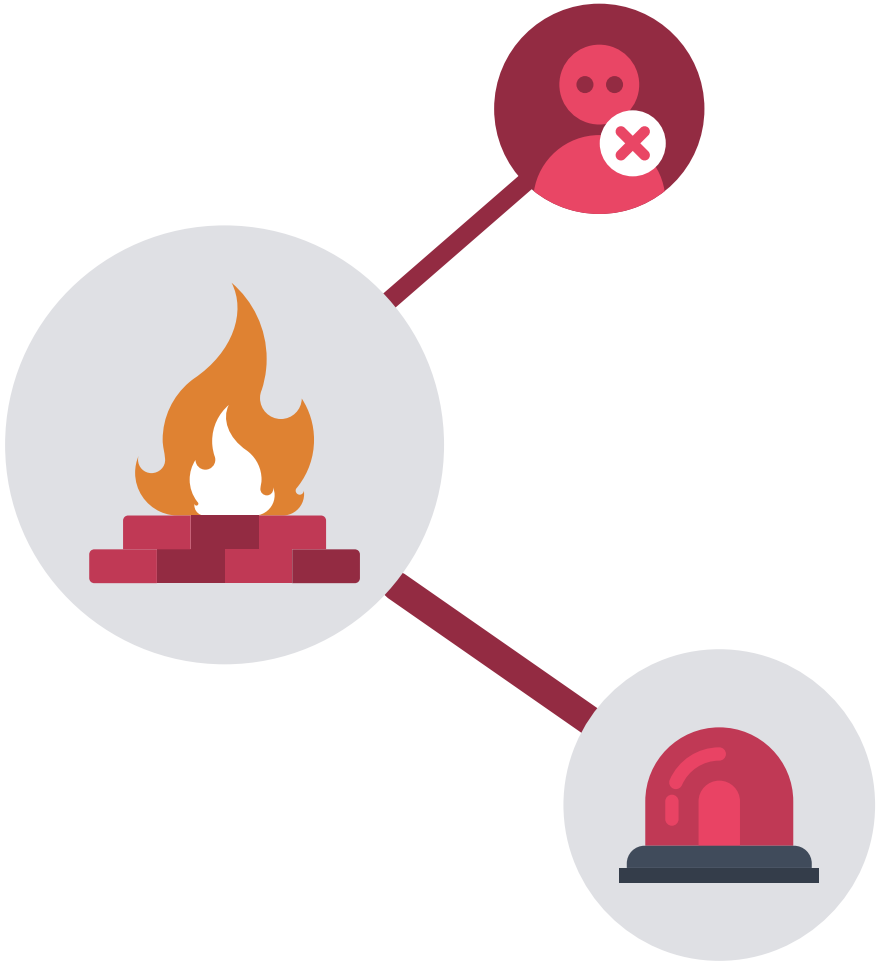
Deși angajarea unui expert este o idee bună, fiecare angajat din firmă trebuie instruit cu privire la bunele practici în domeniul securității cibernetice.

Gândiți-vă la colegul care, fără să știe, descarcă un atașament rău intenționat al unui e-mail sau vizitează un site web care nu prezintă siguranță, infectând rețeaua societății cu un program malware care încetinește computerele sau trimite informații sensibile către un infractor cibernetic.

În conformitate cu Raportul din 2016 privind amenințările cibernetice realizat de CyberEdge, organizațiile au clasificat „informarea insuficientă a angajaților cu privire la securitate” drept problema principală care le-a împiedicat să se apere împotriva amenințărilor legate de securitate. Aceasta a surclasat alte aspecte precum „lipsa bugetului” și „lipsa personalului calificat”.[10]

Sursă: [10] Studiu derulat în 2016 de Institutul Ponemon privind costul criminalității cibernetice

4 Avem un program antivirus puternic instalat pe sistemele noastre, așadar suntem bine protejați



Programul antivirus funcționează prin scanarea sistemelor din punct de vedere al programelor de tip malware descărcate de pe site-uri web sau din e-mailuri. Însă atacatorii au la dispoziție alte metode pentru a eluda această protecție.

Atacurile cibernetice care nu pot fi blocate de programul antivirus includ atacuri distribuite de tip refuz serviciu (DDoS), situație în care un site web este inundat cu trafic nedorit, care îl încetinește sau îl face nefuncțional; atacuri web, prin care hackerii injectează coduri rău intenționate într-un site în scopuri precum furtul de date sau spionarea la distanță; și obținerea de acces de către hackeri, prin dispozitive furate.

5 Dacă un intrus pătrunde, vom observa acest lucru imediat

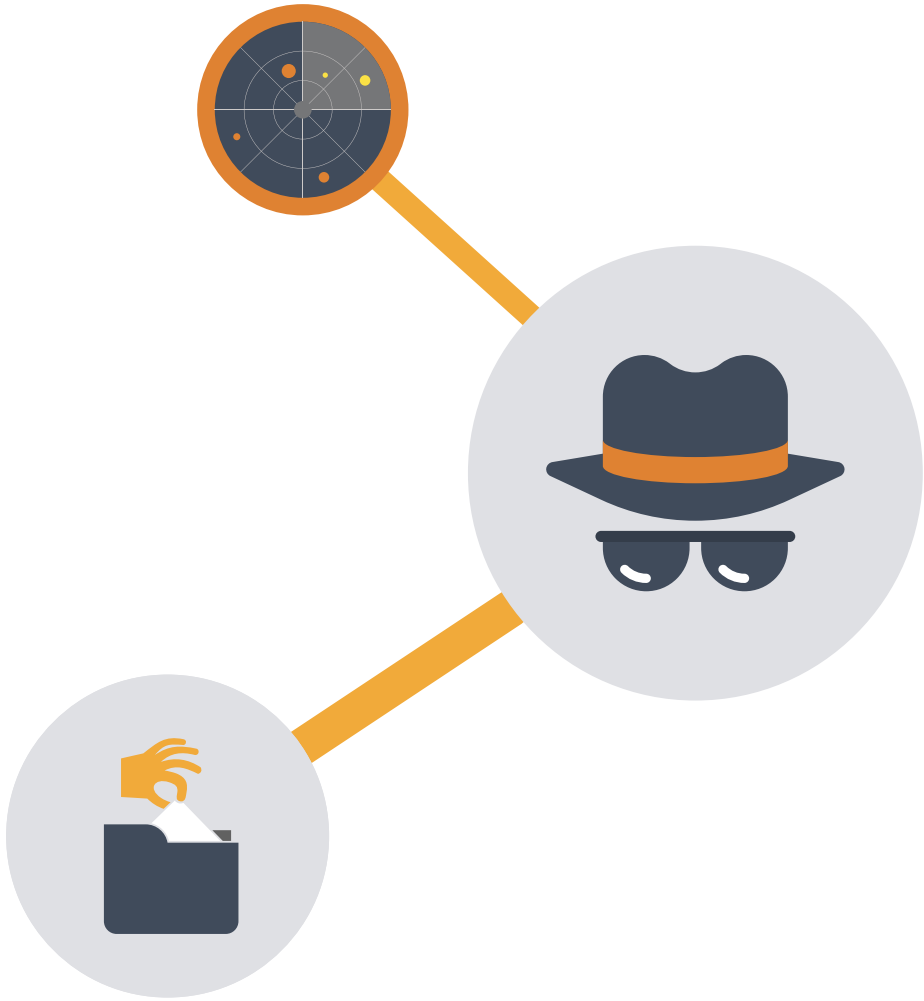
Nu este ușor să detectați un atac cibernetic. Programele malware care intră într-un sistem pot să nu perturbe imediat operațiunile; în schimb, pot spiona sistemul, oferindu-i hackerului informații pentru a planifica atacuri mai bine dirijate, adesea pentru a obține acces în rețea.

Asemenea atacuri asupra unor sisteme specifice sunt categorizate drept amenințări persistente avansate (APA). Atacurile APA sunt caracterizate prin monitorizarea continuă și obținerea de date de la o anumită infrastructură informatică, în timp, de obicei într-un mod nedetectat.

Grupul de consultanță IT Daisy a estimat că jumătate din firmele din Marea Britanie ar putea cădea victimă atacurilor informatice în mai puțin de o oră.

SUGESTIE:
monitorizarea datelor ieșite, pentru determinarea traficului mai mare decât de obicei, poate ajuta la identificarea furtului de date - acesta poate fi un atac APA.

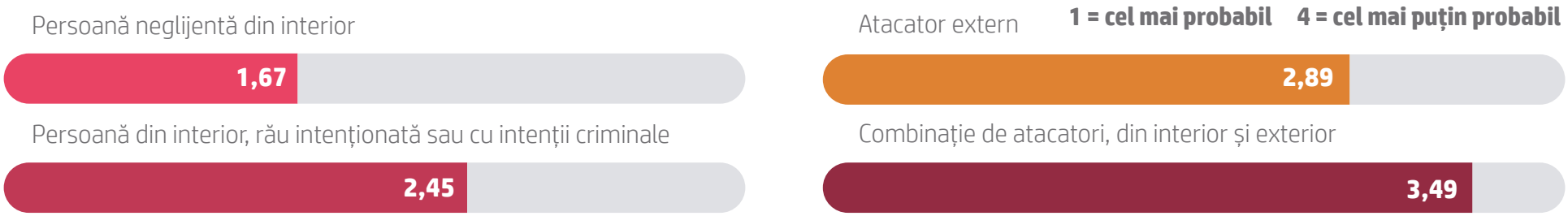
ÎNTREPRINDEȚI ACȚIUNI:
alegeți un software de securitate cu protecție a datelor, precum HP SureStart, care restaurează automat sistemul BIOS al unui computer atunci când se detectează un atac malware - stoparea breșelor înainte ca datele să fie compromise.



De unde provin amenințările?

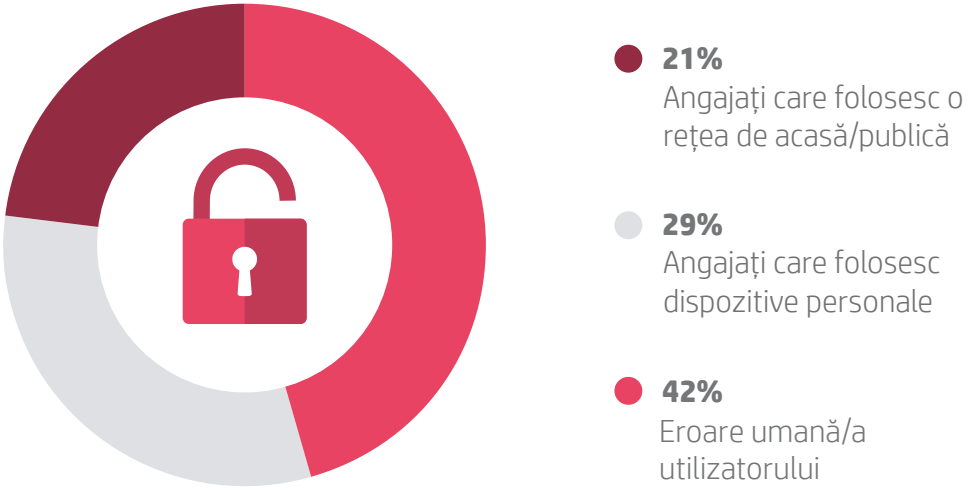
Protejarea rețelei dvs. începe cu cunoașterea punctelor dvs. celor mai slabe

Cea mai probabilă cauză a breșelor de date:[11]



Cele mai obișnuite tipuri de amenințări externe:

Cum se produc breșele interne de securitate: [12]



Surse: [11] http://www.kilpatricktownsend.com/_assets/Kilpatrick%20Townsend%20Report%20Final.pdf [12] Studiul derulat de Institutul Ponemon în 2015 privind costul criminalității cibernetice

Cât costă revenirea în urma unui act de criminalitate cibernetică?

Cele mai costisitoare tipuri de atacuri cibernetice:

25%

1.000.000 £

Coduri rău intenționate și malware

Software care afectează negativ un sistem, creând breșe de securitate, deteriorând fișiere sau furând date (include scripturi, viruși și viermi)

24%

960.000 £

Atacurile tip refuz serviciu distribuit

(DDoS) sunt fluxuri de trafic web care blochează site-ul și serverele unei societăți

16%

640.000 £

Atacuri web

Atacuri care vizează vizitatorii site-ului dvs., precum coduri injectate care redirecționează browserele către site-uri pline cu programe malware

13%

520.000 £

Dispozitive furate

Dispozitivele pierdute ale angajaților care oferă acces la datele de autentificare din cadrul firmei pot conduce la furtul de date și fraudarea identității

9%

360.000 £

Phishing și inginerie socială

E-mailurile sau pop-up-urile care dau impresia unor solicitări legitime de autentificare

9%

360.000 £

Persoane din interior rău intenționate

Angajații care comunică informațiile confidențiale

4%

160.000 £

Sisteme informatice compromise (botneturi)

Rețele de computere infectate care sunt controlate în scopul derulării de activități rău intenționate, spre exemplu trimiterea de mesaje spam

Sursă: [13] Studiu derulat în 2015 de Institutul Ponemon privind costul criminalității cibernetice

Impactul criminalității cibernetice asupra firmelor

Adevăratul cost al criminalității cibernetice îl depășește pe cel al reparării daunelor cauzate de o intruziune

Breșele de securitate sunt incredibil de costisitoare. În sens larg, există trei modalități prin care o breșă poate afecta finanțele firmei dumneavoastră.

Resursele firmei

În mod evident, va trebui să puneți lucrurile în ordine.
Aceasta implică mult timp dedicat de către angajați, precum și costuri semnificative. Ceea ce înseamnă că va trebui să puneți în așteptare alte activități generatoare de venituri.

Amenzi/penalități

Este posibil să primiți o amendă pentru neconformitate (de ex. HIPAA). Odată ce RGPD va intra în vigoare anul viitor la nivelul UE, firmele considerate neglijente ar putea primi o amendă totală de 4% din cifra lor globală de afaceri.
Puteți fi chiar acționat în justiție, dacă scurgerile respective de informații generează o încălcare a protecției datelor clienților.

Reputație afectată în mod negativ

Acesta poate fi unul dintre cele mai nocive impacturi ale unei breșe de securitate.
Clienții, presa și publicul larg reține mult timp breșele de securitate.
Poate dura mult timp până își refac încrederea.

Anatomia intruziunii neașteptate

În momentul în care Sony Pictures a făcut obiectul unei intruziuni în 2014, hackerii pur și simplu „au intrat pe ușa din față”.[14]

Conform personajului „Lena” din grupul de hackeri Guardians of Peace (GOP), care și-au asumat responsabilitatea pentru atac, Sony „nu se mai ocupă de securitatea fizică”. Hackerii au obținut acces la rețeaua Sony intrând fizic în clădire și furând acreditările informatice ale unui administrator de sistem.

Odată ce au intrat, au introdus în sistem programe malware care au accesat fișiere private, coduri sursă și parole pentru bazele de date Oracle și SQL. De acolo, au furat programele producțiilor de filme, e-mailuri, documente financiare și multe altele, și au publicat multe dintre aceste informații online.

Hackerii au amenințat să publice mai multe date secrete și strict secrete dacă compania nu retrage filmul „The Interview” din cinematografe.

În cele din urmă, Sony a capitulat, pierzând încasări despre care nu a oferit informații și, de asemenea, suportând o știrbire incredibilă a reputației sale.

Sony a comis două greșeli. Nu a luat în calcul accesul fizic al intrușilor la datele companiei și nu a investit în mai multe linii de securitate, fapt care ar fi putut preveni accesul la informațiile confidențiale în urma brешei inițiale.

În calitate de expert în securitate, Bruce Schneier a scris după atac că „În fața unui atacator suficient de competent, finanțat și motivat, toate rețelele sunt vulnerabile”. Ceea ce este dificil este să recunoașteți unde anume rețeaua dvs. este vulnerabilă. Poate fi chiar ușa de la intrare.

ÎNTREPRINDEȚI ACȚIUNI:
creați un plan de răspuns în caz de breșă de securitate, pentru fiecare departament, de la IT la Asistență clienți, pentru a minimiza timpul de recuperare.

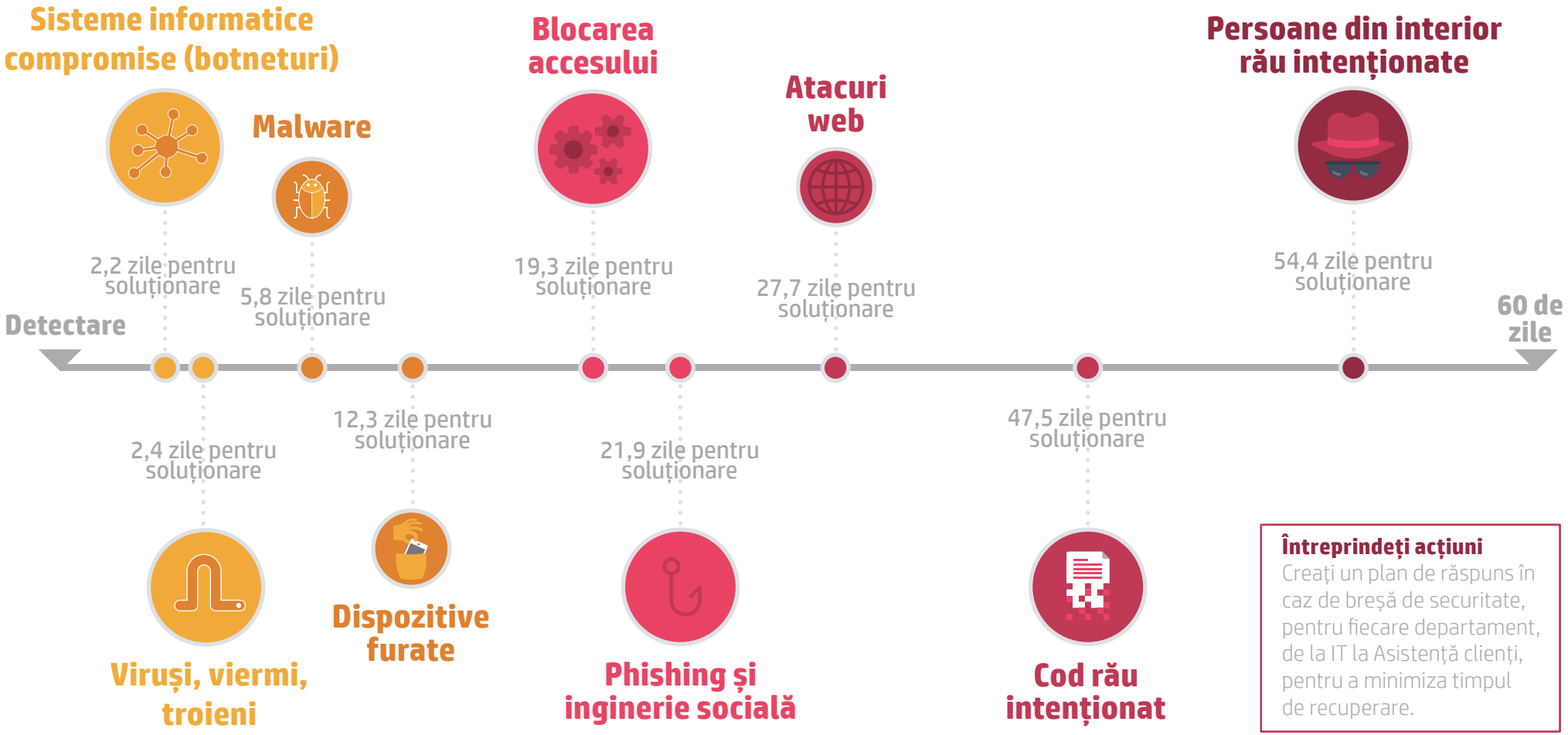
SUGESTIE:
numeroase forme de malware sunt transmise sub formă de atașamente la e-mail. Instruiți personalul să recunoască fișierele suspecte, care sunt concepute să arate ca niște documente legitime.

- Costul estimat al criminalității cibernetice pentru firmele din Marea Britanie: 21 de miliarde USD [15]
- Costul mediu al criminalității cibernetice per firmă britanică, în 2016: 5,7 milioane GBP[16]
- Întreprinderi britanice care s-au confruntat cu o breșă de securitate sau cu un atac cibernetic în intervalul 2015-2016: 66%[17]

Surse: [14] http://www.businessinsider.com/how-the-hackers-broke-into-sony-2014-12?IR=T [15] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[16] https://www.statista.com/statistics/293274/average-cyber-crime-costs-to-companies-in-selected-countries/ Statistica este de 7,21 milioane USD - a fost convertită în GBP
[17] https://www.gov.uk/government/news/two-thirds-of-large-uk-businesses-hit-by-cyber-breach-or-attack-in-past-year

Criminalitatea cibernetică: timpul de recuperare

Cât durează repararea daunelor cauzate de o breșă de securitate a datelor? Institutul Ponemon[18] consideră că media este de 46 de zile, o cifră cu potențial devastator pentru IMM-urile britanice care se bazează pe o funcționare fără întrerupere



Întreprindeți acțiuni
Creați un plan de răspuns în caz de breșă de securitate, pentru fiecare departament, de la IT la Asistență clienți, pentru a minimiza timpul de recuperare.

Sursă: [18] Studiu derulat în 2015 de Institutul Ponemon privind costul criminalității cibernetice

Cum să vă protejați afacerea împotriva criminalității cibernetice

Sugestii și strategii esențiale pentru securitatea cibernetică a activității

Acestea sunt șase obiective frecvente pentru hackerii care pătrund în sistemele companiilor, precum și informații despre ce anume puteți face în această privință, în ziua de azi.

Baze de date cu clienți

Servicii cloud

Smartphone-uri și tablete pentru personal

Erori ale angajaților

Internetul obiectelor

Gateway-uri de rețea

Pe măsură ce evoluăm către o lume din ce în ce mai digitală, unde datele capătă o valoare din ce în ce mai mare, criminalitatea cibernetică poate îmbrăca numeroase forme. Infractorii cibernetici caută deseori informații și, dat fiind că există din ce în ce mai multe dispozitive conectate folosite la locul de muncă - de la smartphone-uri și tablete la imprimante WiFi, există un număr din ce în ce mai mare de puncte de acces care pot fi vizate de hackeri.

1 Baze de date cu clienți

Datele financiare sunt departe de a fi singura țintă a atacatorilor - informațiile precum numele și adresele de e-mail pot fi folosite pentru fraudarea identității, trimiterea de mesaje spam sau accesarea neautorizată a altor conturi.

O recompensă majoră pentru hackerii serioși o reprezintă pătrunderea în cadrul firmelor care deservesc firmele mai mari. Gândiți-vă la acest lucru ca la echivalentul digital al intrării prin efracție într-un magazin de bricolaj numai pentru a avea acces la peretele de la subsol, comun cu cel al camerei în care se află seiful unei bănci naționale, aflate în imediata vecinătate.

Odată ce atacatorii au pătruns în sistemul mai mic, sunt mai bine poziționați pentru a obține acces la datele despre clienți deținute de firmele-client mai mari. Cum ar putea fi compromisă baza dvs. de date cu clienți? Virușii, viermii și troienii - descărcați de pe site-uri rău intenționate sau din e-mailuri - pot declanșa codul necesar pentru ca un hacker să poată intra și să fure date.

Cum să protejați datele clienților dumneavoastră

- Folosiți un software de securitate conceput pentru firme care oferă protecție pentru rețea, e-mailuri și la punctele finale.
- Actualizați-vă în permanență software-ul de securitate pentru a bloca programele malware în continuă evoluție.
- Descărcați actualizări software pentru programele dvs. din sistem, deoarece programele mai vechi pot conține vulnerabilități ce pot fi exploatate de atacatori.

2 Servicii cloud

Cum să protejați datele clienților dumneavoastră

- Criptați-vă cele mai importante informații folosind instrumente precum tehnologia Smartcrypt de la PKWARE, care folosește politici de acces pentru a determina complexitatea criptării. În acest mod, utilizatorii autorizați văd datele pe care trebuie să le vadă, iar utilizatorii neautorizați nu văd nimic.
- Creați o parolă puternică pentru contul dvs. cloud. De asemenea, în setările contului dvs. cloud, definiți exact cine poate accesa datele dvs. și ce poate face cu ele.
- Solicitați autentificarea în doi pași - precum un cod pe smartphone și, de asemenea, o parolă - pentru a efectua modificări asupra datelor din cloud, precum descărcarea, ștergerea sau mutarea fișierelor.

Informatica în cloud a devenit o componentă de bază a infrastructurii întreprinderii.

Sondajul derulat de IDG în 2016 privind informatica în cloud[19] a constatat că 70% dintre întreprinderi au cel puțin o parte din infrastructură în cloud, în timp ce Tripwire a constatat că circa 90% folosesc sisteme cloud pentru infrastructură și/sau stocarea de date, inclusiv a datelor deosebit de importante.[20]

Securitatea este, desigur, o preocupare, însă în realitate datele sunt de obicei mai sigure în cloud - atunci când sunt stocate în spații din afara sediului de către o companie a cărei reputație depinde de securitatea respectivelor date.

Din acest motiv, 64% dintre întreprinderile care au răspuns la sondajul Tripwire consideră că sistemul cloud este mai sigur decât sistemele tradiționale.

Din fericire, această încredere își merită reputația, conform sondajului din 2015 al BIS,[21] doar 7% din firme (mari și mici) au suferit o intruziune gravă în serviciile lor cloud, iar aceasta, în general, din cauza permisiunilor de acces sau a parolelor insuficiente. Totuși, un cloud securizat necesită în continuare o administrare internă robustă din punct de vedere al securității. Să ne gândim numai la ușa de la intrare a companiei Sony.

Surse:
[19] https://www.scribd.com/document/329518100/IDG-Enterprise-2016-Cloud-Computing-Survey
[20] https://www.tripwire.com/state-of-security/security-data-protection/enterprise-impressions-of-cloud-security-in-2016/
[21] Sondajul derulat în 2015 asupra întreprinderilor mici. Ministerul pentru Afaceri, Inovare și Competențe

3 Smartphone-uri și tablete pentru personal

Multe persoane își folosesc dispozitivele personale pentru activități profesionale.

Politici privind aducerea propriului dispozitiv (BYOD) instituite de firme, reprezintă o modalitate de a eficientiza smartphone-urile pe care le dețin deja angajații. Această tendință este în creștere, în condițiile în care 53,2% dintre organizații vor implementa o politică BYOD în următorii doi ani.[22] Însă aceste dispozitive pot reprezenta o țintă atrăgătoare pentru hackeri.

Se estimează că una din cinci aplicații Android conține o anumită formă de malware invaziv, care ar putea fi transmis în fișierele și sistemele companiei în vederea monitorizării activității sau a furtului de informații.

Această amenințare crește, în condițiile în are 64,9% dintre organizații afirmă că volumul de amenințări care le vizează dispozitivele mobile a crescut.[23]

Angajații cărora li se fură telefoanele pot de asemenea să reprezinte adevărate uși de intrare pentru hackeri. Un hoț de telefoane poate vinde dispozitivul unui cumpărător de pe piața neagră, care poate prelua de pe acesta informații necesare pentru pătrunderea în interiorul companiei victimei sau în sistemele unui client mai mare. Organizațiile au oferit un calificativ de 3,54 din 5 pentru capacitatea lor de a se apăra împotriva amenințărilor de securitate provenite de pe dispozitivele mobile. Acesta a fost cel mai scăzut calificativ dintre cele atribuite de firmele intervievate pentru originile potențiale ale amenințărilor.[24]

Cum să securizați dispozitivele deținute de angajați

- Instalați un instrument de detectare a amenințărilor, precum X-Ray de la Duo pentru dispozitivele Android, pentru a identifica mai ușor aplicațiile răuvoitoare și codurile suspecte.
- Solicitați-le angajaților să activeze ștergerea de la distanță a datelor (disponibilă gratuit pentru Android, iPhone și Windows Phone și cu abonament pentru BlackBerry), astfel încât, în eventualitatea unei pierderi, să se poată șterge datele confidențiale de natură profesională și personală.
- Solicitați-le angajaților să activeze criptarea dispozitivelor pe smartphone-urile lor, pentru protejarea datelor (acest lucru este activat în mod implicit pe noile telefoane iOS și Android).

Sursă: [22] Raportul CyberEdge din 2016 privind apărarea în cazul amenințărilor cibernetice [23] ibid [24] ibid

4 Erori comise de angajați

Cum să vă ajutați angajații

- Educați-vă angajații cu privire la bunele practici din domeniul securității cibernetice și oferiți sesiuni regulate de instruire pentru a face față celor mai recente amenințări.
- Dezvoltați un protocol de securitate adaptat activității dvs. și tipurilor de date pe care le prelucrați.
- Creați o echipă pentru comunicarea politicii dvs. privind securitatea cibernetică către angajați, precum și către clienți și partenerii de afaceri.

Principiul de bază al securității cibernetice îl reprezintă o bună politică privind parolele și, totuși, 31% dintre cele mai grave breșe de securitate din 2015 au rezultat din incidente legate de personal.

De la „spargerea” parolelor slabe și până la furtul de documente trimise prin e-mail folosind o conexiune nesecurizată sau la un e-mail tip phishing care vizează un anumit angajat, atacatorii exploatează adesea erorile umane.

5 Pregătiți-vă pentru internetul obiectelor

Firma de cercetare IDM previzionează că numărul de dispozitive conectate la internet va fi de 30 de miliarde în 2020, în creștere față de cifra estimată de 13 miliarde.[25]

În timp ce computerele de la birou sunt securizate cel puțin cu parole și, ideal, cu un software de securitate, materialele în așteptarea imprimării și activitățile de imprimare deseori nu sunt protejate de protocoale de securitate similare.

Aceste imprimante nesecurizate - și alte componente hardware aflate în rețea - pot cădea pradă „programelor de detectare" care pot înregistra activitățile de imprimare, precum și traficul în rețea, numele de utilizator și informații despre parole, toate acestea fiind trimise către un server de criminalitate cibernetică.

Trebuie remarcat faptul că intens mediatizata breșă Dyn se pare că a avut legătură cu o rețea de camere CCTV activate prin internet, realizate de o singură companie, XiongMai Technologies. Conform firmei de securitate Flashpoint.

Aceasta ilustrează faptul că fiecare dispozitiv din rețeaua dvs. este un punct final, iar rețeaua dvs. este la fel de puternică precum cel mai puțin securizat dispozitiv din cadru ei. Circa 97% dintre organizații au instituite practici pentru desktopuri/laptopuri, 77% pentru dispozitive mobile și 57% dețin practici de securitate pentru imprimante.[26] Singura modalitate de păstrare a securității este ca toate firmele să dispună de practici de securitate pentru fiecare dispozitiv final.

Cum să vă pregătiți pentru internetul obiectelor

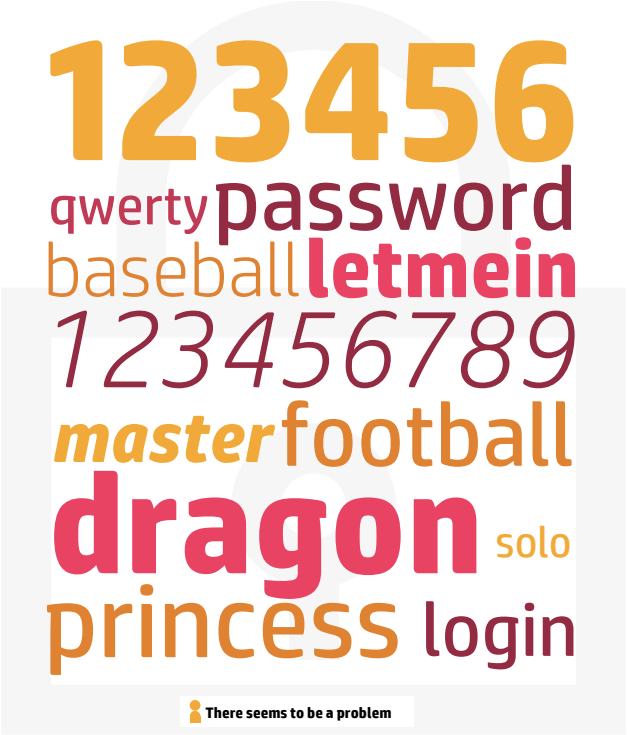
- Eliminați sau dezactivați funcționalitățile de pe hardware care nu sunt utile, deoarece mai multe funcții pot crea mai multe porți de intrare pentru atacatori.

Surse: [25] PwC: Sondajul din 2016 privind situația globală a securității informației [26] Cercetarea privind securitatea imprimantelor HPI, Spiceworks 2016

Parole și programe ransomware

Cele mai obișnuite parole

La începutul anului 2013, un reporter Ars Technica care nu fusese niciodată un infractor cibernetic și nici nu avea experiență în „spargerea” sistemelor protejate prin parolă a decriptat 8.000 din peste 16.000 de parole criptate, într-o singură zi*. Așadar, ce șanse au aceste parole extrem de obișnuite în fața unui hacker hotărât?



Ce sunt programele ransomware

Infractorii cibernetici recurg din ce în ce mai mult la programe ransomware, o formă de programe malware care sabotează sistemele, acestea putând fi ulterior deblocate numai după plata unei răscumpărări în bitcoin. Mii de persoane au fost afectate în urma acțiunii pe scară largă, în 2013, a unui troian numit Cryptolocker, care a atras atenția Agenției Naționale împotriva Criminalității (National Crime Agency) din Marea Britanie și a diviziei sale de criminalitate cibernetică națională. Iată o analiză mai detaliată a modului în care funcționează aceste tipuri de atacuri.

1. Instalare	Codul rău intenționat pătrunde în computerul dvs. după o descărcare neintenționată, printr-un e-mail sau un site web rău intenționat.
2. Notificarea sediului central	Programul ransomware se conectează cu serverul de origine pentru a stabili o cheie de criptare.
3. Vă criptează fișierele	Programul ransomware scanează fișierele din rețeaua dvs. și le criptează, făcându-le inaccesibile.
4. Extorcarea	De obicei, apare un mesaj pe computerul utilizatorului care afișează o limită temporală și o sumă ce trebuie plătită pentru a decripta fișierele înainte de a fi șterse.
5. Efectuarea unei plăți	Antreprenorii vor achiziționa o monedă digitală, precum bitcoin, pentru a o transfera către atacator, care, să sperăm, va decripta fișierele.

* Splashdata

6 Gateway-uri de rețea

Atunci când hackerii doresc să pătrundă într-o rețea, pot declanșa un atac DDoS: mii de aparate infectate cu malware sunt unite pentru a genera atât de mult trafic nedorit, încât rețelele cedează sub amploarea atacului.

Adesea, atacatorii DDoS doresc să distragă atenția administratorilor de site-uri blocând sistemul, în timp ce fură date sau instalează malware pentru a planifica furturi viitoare de date. Unele atacuri sunt de asemenea rezultatul unor hackeri novici, care pur și simplu doresc să facă un site web să devină nefuncțional din simplul motiv că pot face acest lucru. Chiar și câteva ore de nefuncționare a unui site web pot avea consecințe devastatoare pentru rezultatele și reputația unei firme.

SUGESTIE:
investiți în componente hardware care oferă protecție integrată, precum autentificare avansată și instrumente de criptare.

Cum să vă securizați rețeaua

- Implementați sisteme care să verifice traficul intrat și ieșit din rețeaua dvs. O creștere subită ar putea indica un atac, în timp ce o activitate constantă, însă inexplicabilă, ar putea sugera faptul că un troian transmite datele către serverele de origine.
- Filtrați tot traficul, astfel încât numai traficul necesar susținerii activității dvs. să ajungă în rețea.
- Asigurați-vă că fiecare router, switch sau alte dispozitive din rețea funcționează cu același software de bază și caracteristici și descărcați întotdeauna actualizări software.

Viitorul securității cibernetice pentru firme

Dat fiind că firmele au devenit atât de interdependente, este din ce în ce mai important să își construiască mecanisme solide de apărare și securitate cibernetică.

În prezent, angajații își aduc la serviciu propriile lor dispozitive. Firmele folosesc platforme de informatică în cloud și externalizează servicii tehnice foarte importante. Și din ce în ce mai multe persoane lucrează acum de la distanță. Securitatea cibernetică acționează agregat atunci când nu controlați nici dispozitivul, nici infrastructura și nici spațiul de lucru.

În același timp, smartphone-urile ne-au învățat că activitatea se poate desfășura oriunde și oricând. O cafenea reprezintă un spațiu de lucru la fel de bun ca și un birou. Folosim rețele WiFi publice pentru a prelucra cantități enorme de date profesionale și cu caracter personal, adesea prin smartphone-uri care sunt slab securizate. Cu siguranță, infractorii au remarcat deja tendințele. Securitatea are de suferit atunci când nu ținem seama de circumstanțele muncii noastre.

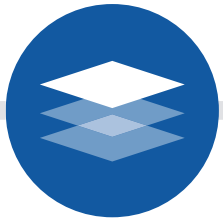
În anii ce vor urma, aceasta va însemna mult mai mult decât adăugarea unui program antivirus la dispozitivele noastre sau actualizarea parolelor la fiecare șase luni. Mai degrabă, firmele trebuie să adopte măsuri de securitate sporite, care funcționează la fel de bine la distanță, cât și într-un birou supervizat de un administrator IT

Pentru organizațiile distribuite din ziua de mâine, securitatea cibernetică depinde de instrumente de analiză sofisticate, care izolează comportamentul neobișnuit, precum și de o securitate care acționează pe mai multe fronturi, protejând toate punctele de acces.

Viitorul securității cibernetice pentru firme

Analiză: detectivul în securitate cibernetică

Deși site-ul dvs. nu are un trafic intens, va avea anumite modele. Folosirea instrumentelor de analiză care măsoară și jurnalizează activitatea pot facilita diagnosticarea, în cazul în care ceva nu funcționează adecvat. Aceste instrumente acționează mai întâi prin urmărirea și documentarea comportamentului normal, pentru a detecta ulterior anomaliile. Odată detectate, administratorii pot iniția ofensiva și îndepărta atacurile înainte ca ele să aibă ocazia de a dezlănțui haosul cibernetic.



Mai multe straturi: atacatorii trebuie să rămână cu un pas în urmă

Numită uneori „apărare în profunzime”, securitatea structurată pe linii multiple de apărare protejează fiecare punct de acces în mai multe moduri. Abordările cele mai obișnuite includ certificate SSL cu validare prelungită, care îngreunează falsificarea acreditărilor necesare pentru a intra într-o rețea securizată. Sprijinirea acestei măsuri cu autentificarea multifactorială care le impune invadatorilor să „spargă” mai mult de o singură parolă poate fi, de asemenea, utilă.

Indiferent de tehnologia specifică folosită, principiul din spatele liniilor de apărare constă în blocarea în diferite moduri a fiecăreia din zonele sensibile ale rețelei dvs. profesionale. Utilizatorii și partenerii dvs. pot avea nevoie de mai mult timp și efort pentru a accesa date esențiale, însă inconvenientele sunt contrabalansate de siguranța activității dvs.

Întreprindeți acum o acțiune

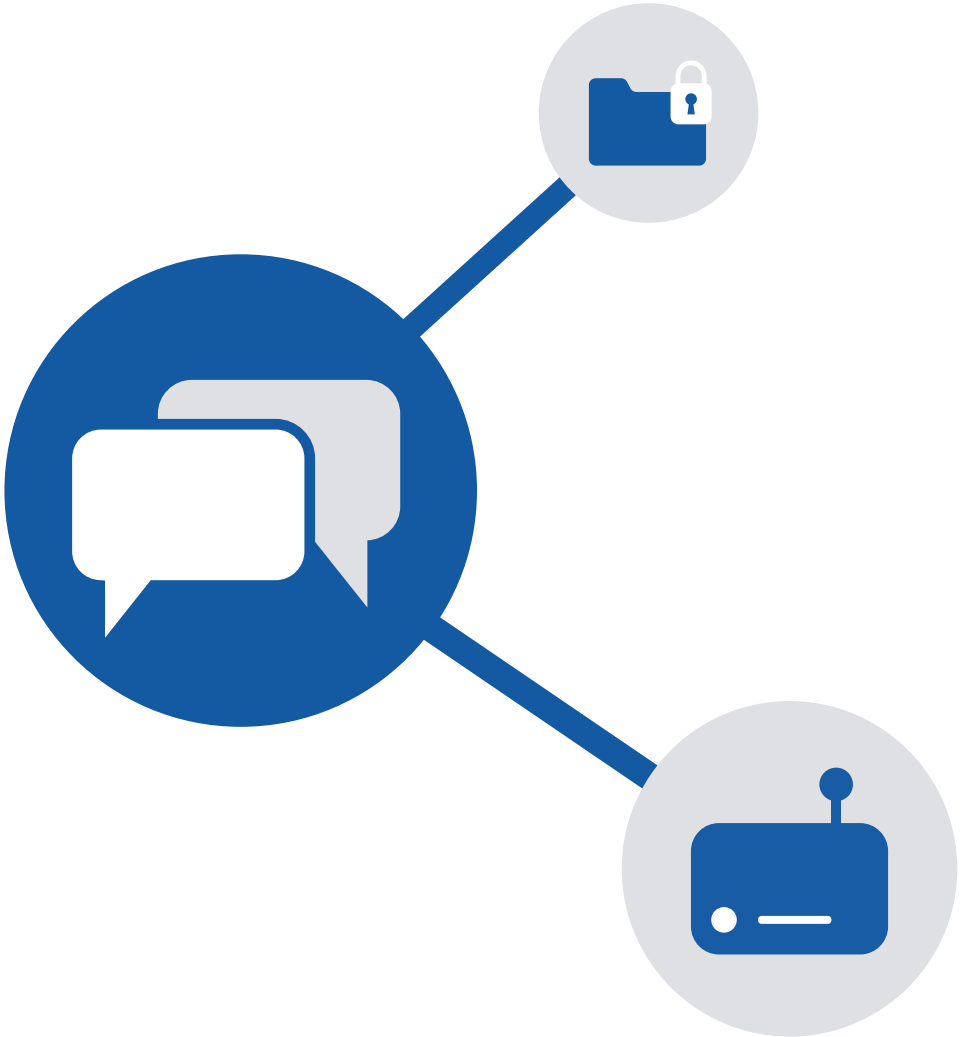
Investirea în software-ul și instruirea din domeniul securității cibernetice reprezintă cea mai bună apărare. Începeți prin a audita sistemele și infrastructura dumneavoastră. Faceți suficiente lucruri? Ce ați putea face mai bine?

În fine, puteți de asemenea să apelați experții noștri de la Hewlett Packard Inc. Baza noastră colectivă de cunoștințe se concentrează pe a fi cu un pas înaintea amenințărilor și nu doar pe răspunsul la ele. Pentru a afla mai multe, vă rugăm să ne vizitați la HP.com.

SUGESTIE:
mai întâi urmăriți și documentați comportamentul normal pentru a putea detecta ulterior anomaliile.

Considerente privind securitatea dispozitivului final

Securizarea fiecărui dispozitiv din rețeaua dumneavoastră



Cercetările din domeniul securității derulate de Spiceworks[27] au constatat că principala sursă de amenințări de securitate cu care se confruntă firmele o reprezintă:

- laptopurile și desktopurile: 81% externe și 80% interne
- dispozitivele mobile: 36% externe și 38% interne
- imprimante 16% externe și 16% interne

Care dintre aceste amenințări trebuie securizată cel mai urgent? Răspunsul cel mai simplu ar fi toate. Deși acest lucru poate fi evident, un număr alarmant de organizații încă mai aleg ce dispozitive să securizeze.

Perspectiva HP este că orice dispozitiv care se conectează la rețeaua dvs. trebuie securizat. Sau, reformulat mai simplu: rețeaua dvs. este la fel de sigură ca cel mai puțin securizat dispozitiv din cadrul ei.

Logica intuitivă vă poate spune că securizarea unei imprimante conectate nu este la fel de importantă ca securizarea flotei de laptopuri. Însă riscul este similar. Se știe că hackerii vizează lucruri precum imprimantele sau orice dispozitiv inteligent care se conectează la rețeaua dvs. Ei știu că aceste dispozitive nu sunt, de obicei, foarte bine securizate, însă oferă același nivel de acces la rețeaua dvs.

Sursă: [27] Cercetarea HP din 2016 privind securitatea imprimantelor, Spiceworks

HP: Deschidem drumurile într-un domeniu complet nou

Securitatea cibernetică este în schimbare. Avem instrumentele necesare pentru a vă ajuta să vă apărați.

Nu există remedii rapide în securitatea cibernetică. O apărare solidă necesită o abordare compusă din mai multe fațete, care include rețele, dispozitive și oameni. Alegerea tehnologiei adecvate este un bun început.

La HP, siguranța este pe primul loc. Gama de dispozitive HP Premium Elite oferă funcționalități de securitate de top în domeniu, care nu mai sunt oferite de alți producători, spre exemplu HP SureStart - primul BIOS cu reparare automată din lume.

HP își echipează dispozitivele cu:

- **blocaj Bluetooth:** folosind tehnologia Bluetooth, dispozitivul se blochează automat atunci când vă îndepărtați de el și se deblochează când reveniți.
- **securitate biometrică:** recunoașterea facială și a amprentelor oferă acces numai utilizatorilor care s-au autentificat biometric.
- **ecrane HP SureView*:** monitorul închis la culoare nu le permite privitorilor să vadă ecranul dvs., protejând materialele confidențiale atunci când lucrați din afară.
- **BIOS cu reparare automată HP SureStart:** fiecare HP Elite își monitorizează sistemul BIOS la fiecare 15 minute. În momentul în care detectează o anomalie, resetează computerul la starea sa originală, eliminând orice intruși.

Gama Elite de la HP nu vă va proteja singură activitatea. Însă va construi o primă linie puternică. Vizitați www8.hp.com pentru a afla mai multe despre gama completă HP Elite.

* La modelele selectate

HP: Suntem pionieri în domeniul imprimării

Protejați-vă rețeaua folosind cele mai sigure soluții de imprimare din lume*

„Grație angajamentului pe termen lung față de securitatea imprimării, HP deține cel mai amplu și complex portofoliu de soluții și servicii de securitate de pe piață”.

– Quocirca, ianuarie 2017**

HP își echipează dispozitivele cu:

- **Funcție de detectare a intruziunilor în momentul rulării:** Funcția HP de detectare a intruziunilor în momentul rulării ajută la protejarea dispozitivelor în timp ce funcționează și sunt conectate la o rețea - exact momentul în care apar cele mai multe atacuri.

- **Manager de securitate Jet Advantage:** Acesta le oferă administratorilor de sistem o abordare eficientă pentru a evalua și, dacă este necesar, pentru a îmbunătăți setările de securitate ale dispozitivelor din întreaga rețea, astfel încât să respecte politicile de securitate stabilite de companie.

- **BIOS cu reparare automată HP SureStart:** La repornirea sistemului, HP SureStart detectează și previne executarea codurilor rău intenționate, iar BIOS-ul se repară automat. Se reîncarcă folosind o copie „de aur” integrată

- **Stabilirea unei liste albe:** Permite încărcarea în memorie doar a codurilor autentice, verificate de HP. Dacă este detectată o anomalie, dispozitivul repornește în stare offline securizată și trimite o notificare departamentului IT.

Surse: *Oferim 5 „cele mai sigure soluții de imprimare”, conform analizei HP a caracteristicilor de securitate publicate în 2016 pentru imprimante competitive din aceeași clasă. HP este singura companie care oferă caracteristici de securitate care pot detecta și opri automat un atac, iar apoi pot valida automat integritatea software-ului la repornire. **Quocirca, „Securitatea imprimării: o cerință obligatorie în era IoT”, quocirca.com/content/print-security-imperative-iot-era, ianuarie 2017.

Glosar și informații suplimentare

Instrumente de administrare a accesului

Botnet:
se referă în general la un tip de program automat, conceput pentru a accesa și a controla computerele conectate la internet, fără ca proprietarul să aibă cunoștință de acest lucru. Computerele sunt adesea infectate cu malware. Hackerii folosesc botneturi pentru a declanșa un **atac refuz-serviciu (DDoS)** pe un site web.

Instrumente de prevenire a pierderii de date:
o categorie vastă de software având drept scop monitorizarea datelor sensibile și blocarea tentativelor persoanelor neautorizate de a le accesa sau copia. Diferitele abordări permit protecția la punctul de acces (anume, la punctul final), în timpul traversării unei rețele, sau într-un sistem de fișiere. Gartner a previzionat că această piață **urma să crească cu 25%** în 2013.

Tehnologii de criptare:
instrumente care **fac ca datele să devină ilizibile** fără un anumit decodor. În ultimii ani, comisarul britanic pentru informații s-a pronunțat **puternic în favoarea** diferitelor tipuri de criptare. Mai recent, guvernul a fost forțat să **își schimbe diametral poziția cu privire la tehnologia de criptare**, în urma unor critici aspre.

Tehnologiile tip paravan de protecție:
un alt termen larg care descrie un tip de dispozitiv care folosește algoritmi și alte tehnici pentru a bloca traficul neautorizat și accesul utilizatorilor într-o rețea. **Versiunile de următoarea generație** ale acestor dispozitive pot fi foarte puternice, din punct de vedere al modului în care combină funcții ce anterior fuseseră gestionate de dispozitive diferite. Spre exemplu, detectarea intruziunii. De asemenea, tind să țină cont de aplicație și, prin urmare, cunosc diferența dintre traficul web aferent unei implementări salesforce.com și cel aferent unei pagini de Facebook.

Instrumente GRC:
au scopul de a se referi la inițiative extinse și coordonate din interiorul unei societăți, pentru gestionarea și reglementarea operațiunilor într-un mod conform cu normele și care, drept rezultat, reduce riscurile.

Malware:
o categorie extinsă de software care poate afecta negativ sau chiar dezactiva alte sisteme. Virușii, viermii și troienii sunt exemple de malware. De asemenea, în sensul studiului Ponemon citat în acest e-book, programele malware sunt considerate a fi diferite de viruși, aceștia „fiind situați la punctul final și neinfiltrându-se încă într-o rețea”.

Controalele perimetrului:
o categorie generală, care descrie apărarea cibernetică în punctul în care internetul public sau o altă rețea publică se întâlnește cu o rețea privată, gestionată și deținută la nivel local. **Sunt, de obicei, implicate mai multe straturi și tipuri de dispozitive**.

Phishing:
atacuri derulate de obicei prin e-mail, în cadrul cărora un atacator solicită informații de identificare într-o casetă de dialog cu aspect legitim.

Instrumente de gestionare a politicii:
în sensul larg, instrumentele de gestionare a politicii stabilesc un standard pentru ceea ce anumiți utilizatori pot sau nu să vadă și apoi aplică respectiva politică în cadrul unei rețele întregi. Consecvența (cel puțin teoretic) asigură securitatea.

Glosar și informații suplimentare

Sisteme cu informații de securitate:
o gamă largă de informații de securitate care pot ajuta la colectarea și sintetizarea informațiilor legate de amenințări. Sistemele diferă, de la programe de gestionare a jurnalelor la sisteme pentru detectarea anomaliilor în rețea.

Inginerie socială:
în acest caz, atacatorul acționează pentru a constrânge un utilizator autorizat să comunice informații pe care nu ar trebui să le dezvăluie, acordându-i astfel acces atacatorului.

Cal troian:
având un impact similar virusului sau viermelui, calul troian trebuie instalat de utilizator și, ca atare, are tendința de a fi deghizat în mod inteligent. Efectele pot varia, de la schimbarea setărilor computerului, până la ștergerea fișierelor pentru crearea unei „uși din spate” pe care hackerul o poate exploata ulterior.

Viruși:
coduri rău intenționate care sunt capabile de a se multiplica și de a se împrăștia într-o rețea.

Atacuri web:
cel mai adesea, un atac web implică redirecționarea unui browser către un site rău intenționat.

Viermi:
spre deosebire de viruși, care se propagă atunci când se partajează un fișier gazdă, viermii se pot multiplica independent de fișierul gazdă, precum un document Word sau o foaie de calcul Excel și, prin urmare, nu necesită o interacțiune suplimentară cu omul pentru a produce efecte distructive. Sistemele de mesagerie instantanee sunt recunoscute pentru faptul că împrăștie viermi; Skype s-a aflat într-o astfel de situație neplăcută în anul 2012.

4AA7-1085ROE