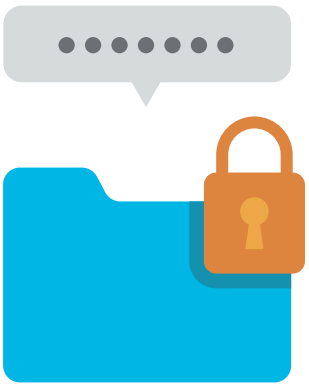
Raport privind activitatea companiei

Securitatea începe la punctul final

Argumente în favoarea acordării de prioritate securității la punctul final

Oferit de

Rezumat



82% dintre organizații s-au confruntat cu o amenințare/breșă de securitate cibernetică în ultimele 12 luni.[1] Criminalitatea cibernetică capătă o amploare din ce în ce mai mare din punct de vedere al frecvenței atacurilor, al gravității și al costului acestora.

Paradigma securității bazate pe prevenție și protecție - apărarea unui perimetru de rețea protejat printr-un paravan de protecție - nu mai este de actualitate. Detectarea și răspunsul sunt cu mult mai eficiente.

Însă bugetele IT nu reușesc să țină pasul cu peisajul în continuă transformare al securității cibernetice. 77% din cheltuieli sunt încă direcționate spre prevenire și protecție.[2] Numai 36% dintre managerii de securitate IT consideră că dispun de un buget amplu pentru o securitate eficientă la punctul final.[3]

Este posibilă o protecție robustă a datelor. Cu tehnologia adecvată - de la soluții de securitate bazate pe detecție și răspuns până la dispozitive individuale - ci strategia corectă și cu resurse suficiente, organizațiile se pot proteja împotriva criminalității cibernetice.

Incapacitatea de a majora investițiile în securitatea cibernetică și de a realinia investițiile pentru o apărare cu adevărat eficientă va avea ca rezultat o frecvență sporită a breșelor de securitate, generând un cost sporit pentru organizație.

Introducere

Securitatea cibernetică în era rețelelor amorfe
60% dintre managerii IT consideră că volumul sporit și nivelul de sofisticare al criminalității cibernetice depășește metodele lor de apărare. 80% dintre responsabilii de securitate consideră că amenințările reprezentate de APA-uri (amenințări persistente avansate), întreprinderi criminale, hackeri și hacktiviști sponsorizați de stat sunt în creștere și reprezintă principala provocare cu care se confruntă securitatea IT.[4]

Și nu se înșală. În Marea Britanie, guvernul estimează costul economic al criminalității cibernetice la 27 de miliarde GBP, o cifră „semnificativă și care probabil că va crește", iar pierderile înregistrate de firme sunt considerate a fi de 21 de miliarde GBP.[5] În Raportul Ponemon din 2016 privind starea dispozitivelor finale, 78% dintre firme au raportat o creștere a gravității atacurilor malware, de la 47% în 2011.

Însă accentul pe amenințările externe este oarecum greșit direcționat și poate conduce la o concentrare inadecvată a resurselor în prevenirea și protejarea apărării de perimetru.

Deși atacurile externe - viruși, malware, phishing - sunt mai prevalente, atacurile din interior sunt mai costisitoare.[6] Și multe dintre aceste atacuri externe provin din vulnerabilități interne; angajați neglijenți care ignoră protocoalele de securitate, dispozitive nesecurizate conectate la rețea - lucru pe care 81% dintre respondenții la sondajul Ponemon l-au identificat ca reprezentând cea mai mare amenințare la adresa securității IT.

Acest lucru se va materializa din ce în ce mai mult odată cu trecerea timpului. Punctul final este cea mai slabă verigă a oricărei rețele și, odată cu răspândirea BYOD, a lucrului la distanță și a internetului obiectelor, punctele finale se înmulțesc. Aceasta înseamnă că numărul de căi de acces pentru hackeri crește la rândul său.

Departe de rețelele controlate de odinioară, compuse din computere desktop legate la Ethernet, rețelele profesionale au devenit amorfe, un hățiș de dispozitive profesionale și personale, care accesează date prin mai multe noduri WiFi, atât în interiorul sediilor, cât și în afara acestora.

Situația nu este insurmontabilă. Esența constă în adoptarea unei noi abordări în privința securității cibernetice. A unor noi strategii care să răspundă la peisajul în continuă schimbare al criminalității cibernetice. A unei noi tehnologii, capabile să diminueze nivelul sporit de sofisticare al unei amenințări în creștere.

În acest raport, înainte de a aborda aspectul securității cibernetice în era dispozitivelor multiple, vom examina natura și amploarea amenințării rețelelor nesecurizate și a sistemelor cloud.

[1] Cercetarea din 2016 privind securitatea imprimantelor HPI (Spiceworks)
[2] Managementul răspunsului la incidentele PAC, 2015: https://www.pac-online.com/download/19443/155514
[3] Raportul Ponemon din 2016 privind starea punctelor finale
[4] Evaluarea IBM CISO din 2014
[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[6] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic

Amploarea amenințării

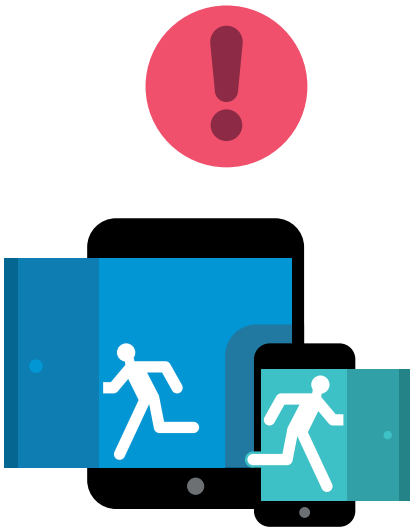
Revenirea în urma breșelor obișnuite de informații costă firmele 907.053 USD, pe lângă o pierdere de 13% a veniturilor. În medie, unei organizații i-ar lua nouă săptămâni pentru a-și reveni.[7]

Aproximativ 85% dintre firmele care au participat la sondajul ce a stat la baza Raportului privind securitatea imprimantelor HP din 2015 au afirmat că s-au confruntat cu o amenințare/breșă de securitate în ultimele 12 luni. 80% dintre profesioniștii IT intervievați anticipează că amenințarea va crește în următorii trei ani.[8]

Criminalitatea cibernetică implică cheltuieli importante. Valoare pierdută din cauza a ceea ce este furat sau avariat. Venituri pierdute din cauza știrbirii reputației și productivitate pierdută. Resurse pierdute, cheltuite pentru recuperare - timp petrecut cu Biroul de asistență, implementarea unor noi politici de securitate, pierdere de personal și alte răspunsuri interne. Amenzi și penalități impuse de autoritățile de reglementare. O scădere a prețului acțiunilor.

Amenințarea va crește odată cu numărul de dispozitive conectate la rețea. Datorită internetului obiectelor, Gartner anticipează că până în 2018 vor exista 11,4 miliarde de dispozitive conectate, în creștere de la 6,4 miliarde în 2016. Până în 2020, peste 25% dintre atacurile identificate în cadrul întreprinderilor vor avea legătură cu internetul obiectelor, însă internetului obiectelor i se vor dedica mai puțin de 10% din bugetele de securitate.[9]

Amenințarea criminalității cibernetice este mare și crește în permanență.



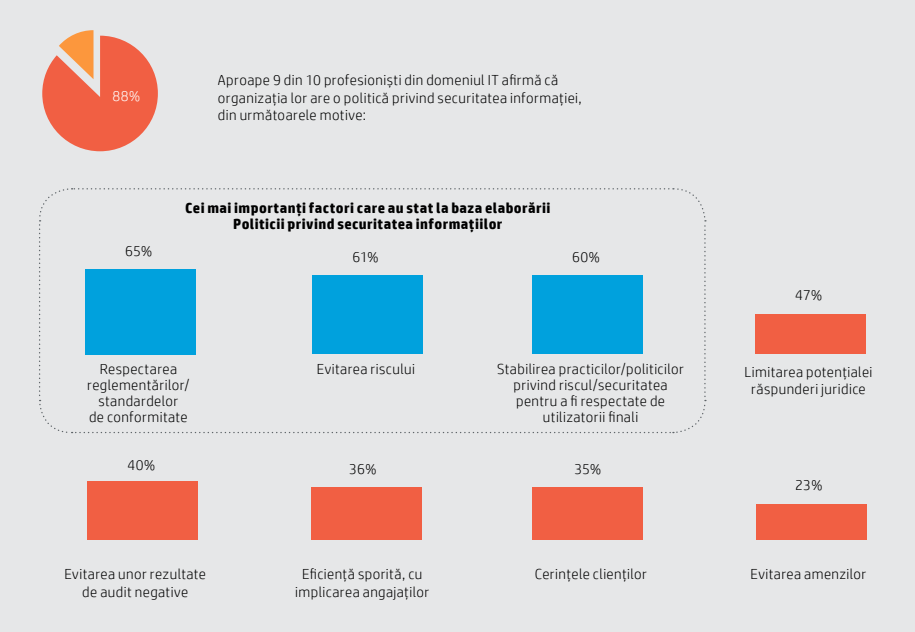
Forma amenințării

Firmele sunt asaltate de nenumărate atacuri cibernetice în fiecare zi. Majoritatea sunt atacuri de nivel scăzut, cu viruși și programe malware. 99% dintre organizațiile intervievate de Ponemon în 2016 se confruntaseră cu programe malware în ultimele 12 luni. Atacurile web externe precum acestea sunt relativ benigne, costând organizațiile, în medie, 4.639 USD.[10]

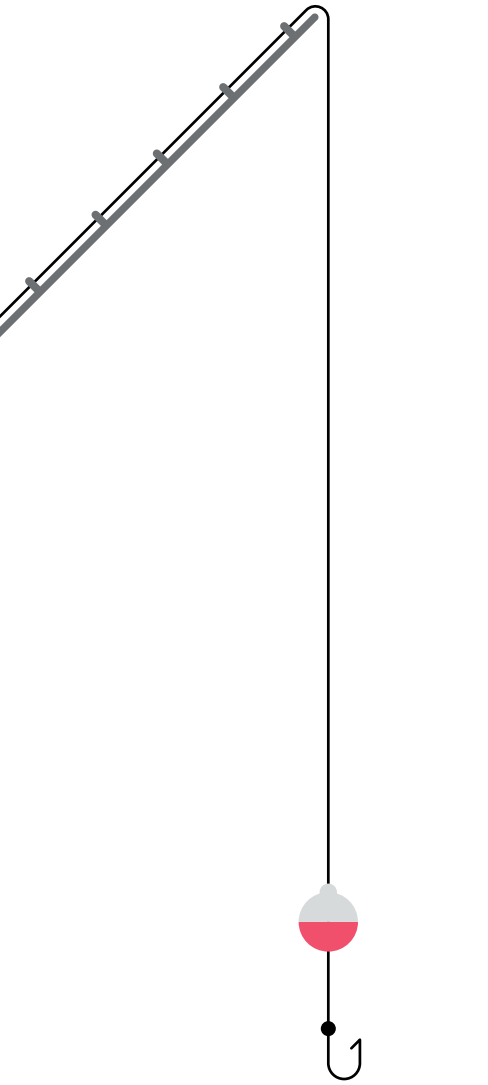
Însă atacurile mai grave sunt din ce în ce mai obișnuite. 51% dintre organizațiile intervievate în 2015 se confruntaseră cu atacuri refuz serviciu (DDoS), care pot avea consecințe foarte grave, costând în medie 127.000 USD. Un fapt și mai alarmant este că 35% dintre ele se confruntaseră cu un atac rău intenționat din interior, care a costat în medie 145.000 USD.[9]

Imaginea pe care ne-o putem construi este a unor atacuri minore neîncetate din exterior, combinată cu atacuri majore, sporadice, însă extrem de probabile; care sunt probabil favorizate de neglijența, dacă nu reaua intenție, din interior. 62% dintre organizații se confruntaseră anterior cu atacuri tip phishing/inginerie socială, care au exploatat slăbiciunile angajaților și care au implicat un cost mediu de 86.000 USD[11]

Un sondaj separat derulat de Spiceworks, în numele HP, a împărțit atacurile suportate în 2014-2015 la 90 de organizații din Marea Britanie.[12]



[7] Riscul de securitate NTT: raportul din 2016 privind valoarea
[8] Raportul din 2015 privind securitatea imprimantelor HP
[9] http://www.gartner.com/newsroom/id/3291817
[10] https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-8392enw.pdf
[11] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic
[12] Cercetare privind securitatea imprimantelor HPI, derulată de Spiceworks în 2016



Cum se produc breșele

Titlurile de pe prima pagină a ziarelor portretizează hackeri întreprinzători, care reușesc să depășească rețele securizate sofisticate ale guvernelor și întreprinderilor, însă realitatea este, de obicei, mai temperată.

Virușii pot profita de pe urma rețelelor compromise, însă programele malware au nevoie de obicei de o oarecare formă de eroare din partea utilizatorilor. Atacurile tip phishing/inginerie socială depind de aceste erori. Atacurile ample tip DDoS și care au ca scop furtul de informații rezultă adesea și din neglijența utilizatorilor.

Faimoasa intruziune Dropbox se pare că a fost cauzată de un angajat neglijent al companiei Dropbox, care a folosit aceeași parolă pentru sistemele interne și pentru contul său LinkedIn.[13] Aparenta intruziune rusă în DNC se consideră că a fost cauzată de John Podesta, fost consilier al dnei Clinton, care a făcut clic pe un link dintr-un e-mail tip phishing considerat în mod greșit a fi fost legitim de către un consilier.[14]

Hackerii nu au nevoie de asistență activă pentru a reuși. La fel de periculoasă este ignorarea sau minimalizarea importanței protocoalelor de securitate. O amenințare din ce în ce mai mare este cauzată de faptul că angajații își aduc la serviciu propriile dispozitive și folosesc programe de tip cloud, în ambele situații introducându-se elemente nesecurizate într-o rețea de altminteri securizată, fără a fi sub controlul departamentului IT și creându-se o vulnerabilitate nedepistată.

În marea parte a timpului, hackerii nu au nevoie să folosească algoritmi sofisticați sau tehnologie de nișă, ci au doar nevoie ca unul dintre noi să fie puțin neglijent.

Paravanul de protecție este nefuncțional

Piatra de temelie a securității cibernetice a fost reprezentată, până de curând, de programe antivirus și tip paravan de protecție. Prevenire și protejare. Crearea unui perimetru securizat. În mediul profesional actual, aceasta pur și simplu nu este o strategie credibilă.

81% dintre respondenții la studiul Ponemon afirmă că dispozitivele mobile din rețeaua lor au făcut obiectul atacurilor malware. Alți factori care au augmentat riscurile de securitate includ utilizarea de către angajați a aplicațiilor cloud comerciale - menționate de 72% dintre respondenți - BYOD (69%) și faptul că angajații lucrează de acasă și din locații din afara sediilor (62%).[15]

Altfel spus, un paravan de protecție are sens atunci când, în calitate de administrator de rețea, puteți controla ce dispozitive sunt conectate. Însă, într-o perioadă în care angajații își aduc la serviciu propriile lor dispozitive - de obicei mai multe și deseori fără informarea departamentului IT - și din ce în ce mai mulți angajați se conectează de la distanță, pur și simplu nu mai puteți proteja perimetrul. Fiecare dispozitiv neaprobat este un punct final vulnerabil, pe care hackerii îl pot exploata.

[13] https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach

[14] https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0

[15] Raportul Ponemon din 2016 privind starea punctelor finale

Perspectiva HP: să acționăm dincolo de securitatea rețelei

Michael Howard, manager global în practica securității la HP, despre asigurarea securității la punctul final

O preocupare foarte importantă și actuală o reprezintă faptul că firmele au dificultăți să securizeze fiecare punct final din cauza faptului că nu au cunoștințe referitoare la anumite dispozitive și la riscurile pe care acestea le generează. Se simt în siguranță în spatele unui paravan de protecție, în ciuda faptului că acesta nu mai este suficient pentru a proteja împotriva unui atac. Echipele de securitate trebuie să cunoască fiecare punct final din infrastructură și să se asigure că fiecare punct final are mai multe straturi de protecție pentru a proteja împotriva atacurilor din ce în ce mai sofisticate.

Este esențial ca echipele de securitate să investigheze fiecare detaliu al infrastructurii lor IT profesionale și să creeze un strat suplimentar de protecție, pe lângă perimetrele standard de rețea. Numai paravanele de protecție nu pot face față atacurilor sofisticate și este absolut necesară o politică de apărare cu mai multe straturi de protecție, la fiecare punct final, pentru a vă asigura că firma dvs. îndeplinește cerințele de reglementare și evită amenzile costisitoare.

Politica HP constă în faptul că, cu fiecare nouă soluție, serviciu sau produs pe care îl dezvoltăm, securitatea va fi primul lucru căruia îi vom acorda atenție. Echipele de dezvoltare știu că trebuie să răspundă la întrebări de securitate și trebuie să știe cum anume vor implementa securitatea în rețea în modul cel mai sigur.

Mai mult ca niciodată, securitatea trebuie să fie o preocupare esențială și nu una accesorie. Aceasta este politica HP de mulți ani.

[16] http://www8.hp.com/us/en/campaign/computersecurity/

[17] IDC Valoarea pentru firme a securității imprimantelor 2015

Securitate stratificată

O nouă abordare cu privire la securitatea cibernetică trebuie să aibă la bază o structură stratificată.
Securitatea rețelelor rămâne importantă, însă aceasta trebuie să fie formată din rețele discrete. Numeroase breșe au la bază o intruziune inițială, care acordă acces la tot ceea ce se află în sistem. Gândiți-vă la eroarea lui John Podesta în privința mesajului phishing. Împărțirea informațiilor sensibile pe mai multe straturi de acces, astfel încât furtul unei chei să nu ducă la cucerirea castelului, este esențială.

Toate dispozitivele trebuie înregistrate. O problemă esențială pentru managerii IT este să se asigure că fiecare dispozitiv conectat la rețea este protejat printr-un software de securitate actualizat cu regularitate, împotriva virușilor, a programelor malware și spyware, și că este scanat cu regularitate pentru depistarea anomaliilor. Este mai bine să se folosească dispozitivele pe post de senzori, colectând informații în timp real pentru a informa cu privire la orice breșe produse asupra perimetrului de rețea din care fac parte.

Trebuie să se instituie o administrare exhaustivă a securității, iar fiecare angajat trebuie să fie instruit în privința protocoalelor de securitate cibernetică. Erorile umane - de la clicul pe legăturile ilicite până la conectarea cu un dispozitiv de consum - reprezintă amenințarea principală la adresa rețelei. Eroarea umană poate fi redusă prin instruire.

Securitatea dispozitivului

Probabil că cea mai mare problemă cu care se confruntă securitatea cibernetică în prezent o reprezintă controlul asupra dispozitivelor care au acces la rețea.
Prima și cea mai simplă soluție, adoptată deseori, este să se instituie rețele WiFi separate pentru vizitatori și angajați, astfel încât dispozitivele externe nesecurizate să nu aibă acces la rețeaua principală. Aceasta merge în paralel cu instruirea angajaților pentru ca ei să poată folosi această rețea pentru dispozitivele lor personale.

Cea de-a doua este să vă asigurați că dețineți controlul asupra dispozitivelor angajaților. Această problemă trebuie să se regăsească în politica societății privind BYOD sau CYOD și este un argument puternic în favoarea CYOD, care oferă mai mult control asupra a ce dispozitive sunt folosite, a alegerii celor care au caracteristici de securitate mai bune, a modului în care sunt configurate și a gestionării și monitorizării acestor dispozitive.

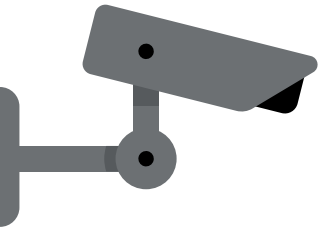
Spre exemplu, folosirea unuia dintre computerele noastre din gama HP Elite este preferabilă folosirii unui laptop ieftin. Fiecare computer HP Elite are încorporată tehnologia SureStart, care verifică sistemul BIOS la fiecare 15 minute și resetează dispozitivul la starea sa originală, în momentul detectării unei anomalii, blocând intrușii nedoriți. Pentru această funcționalitate - și multe altele - computerele din gama noastră HP Elite 800 au fost declarate recent „cele mai securizate computere din lume”.[16] Însă este puțin probabil ca angajații să dețină personal un computer HP Elite.

Angajații preferă deseori să își folosească propriile dispozitive, din două motive:
1. Tehnologia de consum este adesea mai bună decât cea de care dispun la birou
2. Angajaților le place să utilizeze tehnologia pe care o cunosc

Prin oferirea unei politici CYOD bazate pe resurse bune, care să ofere cele mai recente dispozitive actualizate cu regularitate, organizațiile pot pune la dispoziție dispozitive mai bune decât cele deținute de angajați și pot menține un control sporit asupra securității acestor dispozitive. În virtutea acestui principiu HP comercializează dispozitivul ca serviciu (DaaS).

Este esențial să includem toate dispozitivele în strategia de securitate, chiar și cele care sunt, de obicei, uitate. Într-un sondaj IDC, 80% dintre respondenți au afirmat că securitatea IT este importantă pentru activitatea lor, însă doar 59% au admis că și securitatea imprimantelor este importantă, deși mai mult de jumătate se confruntaseră deja în ultimele 12 luni cu o breșă de securitate care implicase securitatea imprimantelor. Acesta este, evident, un lucru trecut cu vederea.

Numărul mediu de breșe de securitate dinaintea implementării unei politici privind securitatea imprimării era de 9,9 per an, la un cost mediu de 521.400 USD (inclusiv amenzi). În urma implementării securității imprimării, numărul mediu de breșe a scăzut la 1,5, ajutând la economisirea a 200 de ore timp de lucru pentru angajați, pe an, și a 250.000 USD, sub formă de costuri conexe, inclusiv audit și conformitate.[17]



Detectare și răspuns proactive

77% din cheltuielile cu securitatea IT se îndreaptă către tehnologiile de prevenire și protecție, precum programe antivirus și paravane de protecție, în conformitate cu cercetările derulate de PAC. Însă această abordare nu este eficientă. Cercetările au constatat de asemenea că 67% dintre firmele intervievate au fost victime ale unei intruziuni cibernetice în ultimele 12 luni, iar 100% dintre ele s-au confruntat cu această situație în trecut.[18]

În special programul antivirus este surprinzător de ineficient. Damballa a derulat teste prin care a atacat deliberat o rețea, pentru a măsura răspunsul antivirus. A durat șase luni înainte ca 100% dintre fișierele rău intenționate să fie identificate.[19] Aceasta susține o altă constatare PAC, conform căreia a durat între o lună și șase luni pentru ca firmele să descopere că fuseseră atacate.

Menținerea securității punctelor finale nu se mai poate baza doar pe prevenire. Numărul în creștere de incidente virus/malware, plus lipsa inerentă de securitate a BYOD/lucrului din afara sediului înseamnă că breșele sunt inevitabile. Nimeni nu sugerează ca prevenția și protecția să fie abandonate în totalitate, însă în mod clar detectarea și răspunsul trebuie să ocupe un loc mai important pe agendă.

Monitorizarea continuă, în timp real, este necesară, folosindu-se, la modul ideal, punctele finale pe post de senzori, aceștia urmând să alerteze restul rețelei în momentul în care a fost compromisă. Aceasta permite asigurarea unui răspuns la distanță oferit de echipa de securitate IT, care să includă procese precum:

- închiderea de la distanță a unui dispozitiv
- stoparea unui proces infectat sau a unuia care împrăștie malware
- punerea în carantină a unui anumit fișier sau grup de fișiere
- perturbarea comunicărilor în rețea pentru a izola dispozitivele infectate[20]

Acceptarea faptului că breșele se vor produce și instituirea unor protocoale adecvate de răspuns, precum și implementarea tehnologiei necesare pentru a le pune în aplicare, reprezintă singura modalitate de asigurare a securității cibernetice, în momentul în care nu ne mai putem baza doar pe prevenție.

„Nicio tehnologie nu poate oferi securitate dacă oamenii o subminează.”

– Joseph Steinberg [21]

Securitatea angajaților

La fel de importantă ca securizarea dispozitivului, dacă nu chiar mai importantă decât aceasta, este securizarea persoanei care îl folosește.
Fiecare angajat trebuie instruit cu privire la securitatea cibernetică. Angajații trebuie să cunoască riscurile implicate de phishing, de navigarea pe site-uri web suspecte, precum și de descărcarea unor atașamente suspecte. Trebuie să cunoască politica privind parolele securizate - folosirea unor parole puternice, unice pentru fiecare autentificare confidențială și folosirea unui manager de parole pentru stocarea lor.

Trebuie informați cu privire la importanța menținerii unui software de securitate actualizat în permanență pe dispozitivele lor, pentru a ușura sarcina de monitorizare a departamentului IT. Trebuie să fie vigilenți și să utilizeze numai dispozitive securizate pentru a accesa rețelele organizației, evitând să folosească dispozitive personale pe rețele externe, nesecurizate, în vederea accesării datelor sensibile.

Mulți experți de renume din domeniul securității cibernetice recomandă rularea unor atacuri phishing simulate - mergând până la construirea unor site-uri web de phishing false, pentru a testa fiecare angajat - și organizând sesiuni de instruire pe tema securității cibernetice la nivel formal. Deoarece majoritatea atacurilor se bazează pe exploatarea slăbiciunilor umane, indiferent dacă este vorba despre neglijență sau rea intenție.

Deoarece oamenii reprezintă cea mai slabă verigă dintre o rețea.

[18] PAC Managementul răspunsului în caz de incident 2015
[19] https://www.damballa.com/time-to-fix-malware-strategies-2/
[20] Lista esențială de verificare pentru detectarea la punctul final – HP acum
[21] https://digitalguardian.com/blog/data-security-experts-answer-what-biggest-misconception-companies-have-about-endpoint-security

Concluzie

Cheltuielile cu securitatea IT ar trebui să treacă de la prevenție și protecție la detectarea și răspunsul la punctul final
Apărarea datelor unei organizații în climatul actual - caracterizat de o criminalitate cibernetică în creștere și de pierderea controlului asupra perimetrului de rețea - necesită două lucruri: o evoluție conceptuală și mai multe resurse.

Conceptul de rețea trebuie să se schimbe. Ideea de rețea concepută ca un gard ce împrejmuiește o serie de dispozitive nu se mai aplică. A sosit momentul să recunoaștem realitatea. „Rețeaua" este o himeră. Ia rezultă din dispozitive conectate, fiecare dintre acestea fiind un punct final. Securizarea rețelei înseamnă securizarea punctului final. Și fiecare punct final se compune din două elemente: dispozitivul și persoana care îl utilizează. Ambele trebuie luate în considerare.

Însă aplicarea securității în această nouă paradigmă este mult mai complicată decât mediul simplu și vechi definit de computere-desktop-conectate-prin-Ethernet. Necesită resurse mai importante, iar acestea trebuie obținute. Circa 61% dintre respondenții la studiul Ponemon confirmă acest lucru.

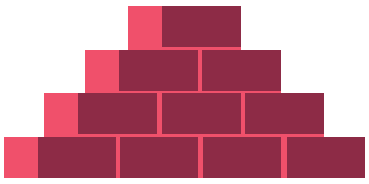
Secretul constă în implicarea restului membrilor organizației. Numai 36% dintre respondenți au considerat că dispun de bugetul și personalul suficient pentru a implementa securitatea la punctul final. 69% au afirmat că departamentul IT nu poate ține pasul cu cererile angajaților vizând o asistență mai extinsă. 71% afirmă că politicile privind securitatea la punctul final sunt greu de aplicat.[22]

80% dintre managerii din domeniul securității IT consideră că respectarea prevederilor legii reprezintă cel mai bun mod de a justifica finanțarea programelor lor de securitate, însă, de asemenea, ei consideră conformitatea ca fiind cel mai puțin important motiv de realizare a cheltuielilor. Conformitatea înseamnă satisfacerea minimului necesar.[23]

Decidenții din domeniul IT trebuie să se coordoneze cu cadrele de conducere executivă pentru a evidenția importanța securității. Explicați clar care sunt costurile unei securități relaxate - cheltuielile de recuperare, veniturile pierdute, valoarea scăzută a acțiunilor - și puneți accentul pe economiile pe termen lung pe care le puteți obține. Numeroase soluții de securitate generează îmbunătățiri și în alte privințe. Gândiți-vă la productivitatea îmbunătățită generată de implementarea securității imprimantelor și la avantajele din punct de vedere al productivității ale oferirii unor sisteme tehnologice actualizate cu regularitate, în cadrul unui program CYOD flexibil, furnizat de entități externe pe bază de abonament (precum DaaS de la HP). Se poate construi o argumentație profesională clară în acest sens.

Provocarea este formidabilă. Și, în timp, odată cu creșterea exponențială a numărului dispozitivelor din era internetului obiectelor și a nivelului de sofisticare sporit al criminalității cibernetice, aceasta va deveni și mai intimidantă. Însă nu este insurmontabilă. Cu tehnologia, strategia, și resursele adecvate, ne putem apăra punctele finale. Ne putem păstra datele în condiții de siguranță.

Pentru a afla mai multe despre Dispozitivele ca serviciu de la HP și despre modul în care vă pot ajuta să derulați un program CYOD exhaustiv, flexibil și securizat, vizitați-ne **aici.**



Abonați-vă pentru a primi actualizări
hp.com/go/getupdated

Distribuiți către colegi

Oferiți un calificativ acestui document

4AA7-1089ROE

[22] Raportul Ponemon din 2016 privind starea punctelor finale
[23] https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697