Departamentele IT si utlizatori individuali, pe masura ce mobilitatea devine tot mai importanta pentru angajati, atunci cand combina munca cu viata personala? Doua studii la nivel mondial releva o imagine reala asupra acestor probleme.

Constatarile Cisco Annual Security Raport (ASR) releva faptul ca cea mai mare concentratie de amenintari la adresa securitatii online nu vizeaza site-urile de pornografie, din domeniul farmaceutic sau jocuri de noroc, in ciuda opiniei generale care a consacrat aceste zone ca cele mai riscante.

De fapt, cele mai multe amenintari tintesc destinatiile legitime vizitate de publicul de masa, cum ar fi marile motoare de cautare, site-urile de cumparaturi si cele de social media.
In comparatie cu un site de sofware contrafacut, site-urile de cumparaturi au o probabilitate de 21 de ori mai mare sa contina amenintari, iar motoarele de cautare sunt de 27 de ori mai susceptibile sa livreze continut daunator. Studiu Cisco
Mai mult, o persoana care acceseaza reclame online are o probabilitate de 182 de ori mai mare de a intalni continut daunator decat accesand site-uri pornografice. Riscurile de securitate sunt in crestere in companii, deoarece multi angajati adopta propriul stil de viata si la locul de munca. Dispozitivele lor, munca prestata si activitatea online se combina cu viata lor personala, indiferent de locul in care se afla – la birou, acasa sau altundeva.

Implicatiile la nivelul securitatii companiilor generate de aceasta tendinta de consum sunt sustinute de concluziile Cisco Connected Technology World Report (CCWTR), care ofera o perspectiva asupra atitudinilor noii generatii de angajati, si anume Generatia Y. Conform studiului citat, majoritatea angajatilor din Generatia Y cred ca mediul online nu asigura confidentialitate (91%), dar numai o treime spun ca nu sunt ingrijorati de faptul ca datele lor personale sunt colectate si stocate.

Ei **sunt dispusi sa-si sacrifice informatiie cu caracter personal pentru a socializa online**.
De fapt, mai multi angajati din Generatia Y au declarat ca se simt mai confortabil sa ofere informatii cu caracter personal site-urilor de cumparaturi online decat departamentului IT al angajatorului – departamente care sunt platite pentru a proteja identitatea angajatilor si dispozitivele acestora. Pe masura ce tot mai multi membri ai Generatiei Y absolva facultatea si intra in randul fortei de munca, politica si cultura companiilor vor fi supuse unor presiuni in crestere. Aceste presiuni se datoreaza cerintelor noii generatii: libertatea accesului pe site-urile de socializare, alegerea dispozitivului de lucru si un
stil
de viata mobil, pe care generatiile anterioare nu l-au solicitat niciodata.
Membrii Generatiei Y verifica in mod constant noutatile de pe site-urile de socializare sau de pe

email, indiferent daca sunt in pat (3 din 4 respondenti), la cina (aproape jumatate), la baie (o treime) sau in timp ce conduc (1 din 5).World Technology Report, decembrie 2012
Acest stil de viata va fi adoptat tot mai mult si la locul de munca, evidentiind felul in care se va lucra in viitor si modul in care companiile ar trebui sa concureze pentru atragerea oamenilor valorosi din noua generatie.

Iata cateva dintre concluziile studiului:

Malware Android

- Malware-ul pentru sistemul Android a inregistat o crestere de 2.577% in 2012.
- Cu toate acestea malware-ul de pe internetul mobil reprezinta doar 0,5% din totalul malware-ului de pe internet.
- Aceste tendinte au devenit deosebit de importante avand in vedere ca smartphone-ul este dispozitivul numarul unu in randul preferintelor angajatilor din Generatia Y, depasind laptop-urile, PC-urile si tabletele (din concluziile primei parti a CCWTR).

Amenintarile malware pe tari Anul 2012 a adus o schimbare semnificativa in ceea ce priveste zonele geografice in care utilizatorii s-au confruntat cu amenintari malware. Astfel, in statistica tarilor cele mai afectate de malware, China a coborat de pe locul 2 in 2011 pana pe locul 6 in 2012.

Tarile scandinave, precum Danemarca si Suedia s-au confruntat un numar mai mare de cazuri de malware pe internet, urcand in clasament pe locul 3, respectiv 4. Statele Unite ale Americii au pastrat locul de lider, cu 33 % din totalul cazurilor de malware de pe internet la nivel global.

Tendintele spam-ului

- Volumul de spam transmis a scazut cu 18% in 2012, comparativ cu anul anterior. Se observa un efort de „eficientizare” a activitatilor de acest fel. Cantitatea de spam transmis la final de saptamana (utilizatori mai putin activi pe e-mail) a scazut cu 25%, iar atacurile sunt concentrate in timpul programului de lucru.
- In 2012, cea mai mare parte a spam-ului a fost trimis in timpul saptamanii (de luni pana vineri), ziua de marti fiind cea mai solicitata din acest punct de vedere.
- India este sursa principala de spam la nivel mondial, iar SUA a trecut pe pozitia a doua in 2012, de pe locul 6 in 2011. Coreea, China si Vietnam intregesc topul primelor 5.
- Cele mai falsificate brand-uri de catre autorii de spam sunt medicamente precum Viagra si Cialis si ceasuri de lux precum Rolex si Omega.
- Spammerii isi maximizeaza rezultatele eforturilor, tintind evenimente reale, cu anumite campanii specifice si de scurta durata.

-ianuarie-martie: software-ul Windows, care a coincis cu lansarea avanpremierei pentru consumatori a Microsoft Windows 8
-februarie-aprilie: software-ul pentru calcularea taxelor in timpul sezonului fiscal din SUA
-ianuarie-martie si septembrie-decembrie: retele profesionale, cum ar fi LinkedIn, corelate cu

dorinta de schimbare a carierei de la inceputul si sfarsitul anului
-septembrie-noiembrie: furnizorii de telefoane mobile, pe marginea lansarii Apple iPhone 5.

Compromiterea confidentialitatii

Cisco a elaborat implicatiile economice ale acestor statistici asupra amenintarilor la adresa securitatii, prin analiza atitudinii si comportamentului angajatilor conectati ai Generatiei Y.

- Desi majoritatea respondentilor din Genetatia Y nu au incredere in modul in care site-urile protejeaza informatiile personale (75%), precum card-ul de credit si datele personale de contact, aceasta lipsa de incredere nu descurajaza comportamentul lor online, ei considerand ca datele lor nu vor fi compromise. Acest lucru pune o mare presiune asupra companiilor, in momentul in care aceste persoane isi asuma riscuri online utilizand dispozitive de lucru conectate la retelele companiilor.
- 57% dintre membri Generatiei Y sunt de acord ca datele lor personale sa fie utilizate de catre site-urile de cumparaturi, site-uri de social media si alte entitati online, in cazul in care acestia vor avea un beneficiu de pe urma acestei experiente.

Respectarea politicii IT

- Noua din zece (90%) profesionisti IT intervievati au declarat ca au o politica ce reglementeaza utilizarea anumitor dispozitive la locul de munca, insa numai doi din cinci respondenti din Geneneratia Y au declarat ca au fost constienti de existenta unei astfel de politici.
- Pentru a inrautati situatia, patru din cinci respondenti din Generatia Y, care au fost constienti de politicile IT, au declarat ca nu se supun acestor politici.
- Profesionistii IT stiu ca multi angajati nu respecta regulile, dar nu sunt constienti de cat de frecvent se intampla acest lucru: Mai mult de jumatate (52%) dintre profesionistii IT considera ca angajatii lor se supun politicii IT, dar aproape 3 din 4 (71%) angajati din Generatia Y declara ca ei nu se supun acestor politici.
- 2 din 3 (66%) angajati respondenti, apartinand Generatiei Y, au declarat ca departamentul IT nu are dreptul de a monitoriza comportamentul lor online, chiar daca ei se conecteaza in retelele companiei cu dispozitivele oferite de companie.
- Aversiunea fata de monitorizarea IT derulata de angajator a fost mai mare decat aversiunea pe care respondentii din Generatia Y au avut-o fata de monitorizarea comportamentului lor de catre site-urile de cumparaturi online. Cu alte cuvinte, Generatia Y se impotriveste mai putin monitorizarii activitatii lor de catre site-urile de cumparaturi, care practic sunt niste necunoscuti, in comparatie cu cea derulata de echipele echipele IT ale propriilor angajatori - echipe care au rolul de a proteja datele lor si ale companiilor.

Internetul tuturor lucrurilor si viitorul securitatii Privind in perspectiva, „Internetul tuturor lucrurilor” reprezinta cea mai mare tendinta online de astazi. Cum din ce in ce mai multe persoane, lucruri si dispozitive se conecteaza la internet, tot mai multe date, din mai multe locuri, vor fi introduse in retelele companiilor si furnizorilor de servicii. Acest lucru va declansa noi vulnerabilitati, precum si nevoia unei abordari mai sofisticate a securitatii.

- Creste zilnic, intr-un ritm exponential, numarul de conexiuni masina-la-masina (M2M) care acceseaza internetul ceea ce va conduce la proliferarea terminalor conectate. Acestea se vor extinde dincolo de aria dispozitivor mobile, laptop-uri si desktop-uri, catre un scenariu "orice-la-orice", in care orice dispozitiv se poate conecta la orice „Cloud”, la orice aplicatie, pe orice retea.
- Pana in 2020, la internet se vor conecta un numar estimat de 50 de miliarde de lucruri, astfel incat numarul de conexiuni va ajunge la mai mult de 13 cvadrilioane (mai exact, 13,311,666,640,184,600). Adaugarea unui singur "lucru" (50 miliarde + 1) va creste numarul de conexiuni potentiale de inca 50 miliarde.
- Aceste noi conexiuni genereaza fluxuri de date mobile care trebuie protejate in timp real, fiind evaluate la nivelul retelei pentru obtinerea de informatii relevante, inainte de a fi compromise si a cauza daune ireparabile
- Pentru profesionistii in securitatea retelei, accentul cade pe infrastructura de transmitere a datelor, trecand de la terminale si echipamente periferice la retea.

„Securitatea retelei si a infrastructurii de transmitere a datelor devine din ce in ce mai importanta, mai ales in contextul in care din ce in ce mai multe dispozitive mobile se conecteaza la retea. Pe de alta parte, cresterea traficului de date datorat in special conexiunilor M2M va pune serios la incercare fiabilitatea tehnologiilor de securitate contextuala si in timp real. In acelesi timp observam o accentuare a atacurilor malware asupra terminalelor cu sistem de operare Android, dar cu toate acestea, atacurile asupra platformelor mobile reprezinta doar 0,5% din totalul acestor amenintari”, spune Cristian Popescu, director General Cisco Romania.

Cisco 2013 Annual Security Report evidentiaza cele mai importante tendinte de securitate ale anului si ofera sfaturi si indrumari pentru a mentine sigure mediile tehnologice din marile companii. Raportul Cisco Connected World Technology aprofundeaza amenintarile prezentate in raportul de securitate.

Cea de-a treia editie anuala Cisco Connected World Technology Report a fost comandata de Cisco si condusa de InsightExpress, o firma independenta de cercetare de piata cu sediul in Statele Unite ale Americii. Studiul consta din doua anchete: una axata pe studenti si lucratori tineri cu varsta intre 18 si 30 de ani, iar a doua s-a axat pe profesionisti IT proveniti din mai multe industrii, la nivel global. Fiecare sondaj include 100 de respondenti din fiecare din cele 18 tari participante la studiu, rezultand un esantion de 3.600 respondenti. Cele 18 tari sunt Statele Unite ale Americii, Canada, Mexic, Brazilia, Argentina, Marea Britanie, Franta, Germania, Olanda, Rusia, Polonia, Turcia, Africa de Sud, India, China, Japonia, Coreea de Sud si Australia.

** sursa : dailybusiness.ro