INTERVIU DORIN PENA (CISCO): HACKING-UL A DEVENIT UN BUSINESS; ESTE ESTIMAT SĂ AJUNGĂ LA 1.000 MILIARDE DOLARI, LA NIVEL MONDIAL, ÎN 2020

(potrivit AGERPRES)

Hacking-ul a ajuns o industrie, un business, fiind evaluat în 2015 la 450 miliarde dolari, la nivel mondial, cu o proiecție de 1.000 de miliarde de dolari în 2020, a declarat, într-un interviu acordat AGERPRES, directorul general al Cisco România, Dorin Pena.

Silviu MATEI / AGERPRES FOTO

Acesta a subliniat că, în România, în ultimii ani s-a ajuns la un nivel mult mai ridicat de înțelegere a riscurilor și de cunoștințe ale oamenilor, însă există un deficit de specialiști calificați în securitatea cibernetică.

Directorul Cisco a mai afirmat că securitatea cibernetică este o prioritate și la nivel european și la nivel național, dar rămâne de văzut cum se va implementa și cum se vor corela legislațiile europene cu cele locale.

AGERPRES: Ministrul Comunicațiilor a declarat recent că Legea securității cibernetice nu este o prioritate pentru el, în timp ce în guvernarea anterioară documentul era considerat prioritate. Din punctul dumneavoastră de vedere, este importantă legea securității cibernetice?

Dorin Pena: Nu aș putea să comentez exact ce s-a schimbat față de anul trecut, în afară de fapte, că s-a schimbat Guvernul și avem un nou ministru. Sunt convins că domnul ministru își înțelege foarte bine prioritățile și le stabilește în urma unui proces intens de analiză. Ce pot să spun este că reglementarea în domeniul securității cibernetice este necesară și utilă. Și sunt pași la nivelul Uniunii Europene, data protection regulation, care, din câte știu, urmează să fie activată în 2018, la începutul anului, la care la un moment dat va trebui să se alinieze și România. Securitatea cibernetică este o prioritate din câte cunoaștem și înțelegem noi și la nivel european și la nivel național. Rămâne de văzut cum se va implementa și cum se vor corela legislațiile europene cu cele locale.

AGERPRES: Directiva NIS (Networking Information Security — n. r.) trebuie implementată anul viitor. Ați fost chemați la consultări? Credeți că deadline-ul poate fi respectat?

Dorin Pena: Dacă e ordin, cu plăcere. La un moment dat, cam asta se va aplica. Din punct de vedere al Cisco, am fost implicați în discuții referitoare la Legea securității cibernetice. Ministerul a fost destul de transparent în a organiza dezbateri, discuții, în a primi un feedback pe variantele vechi ale legii și Cisco, atât direct, cât și prin diverse asociații din care face parte și care exprimă punctul de vedere al mai multor companii și oameni de afaceri din România, a dat părerile sale care, unele s-au regăsit, altele nu s-au regăsit în proiectele anterioare de lege. Acum, nu știu exact, pentru că nu s-au făcut pași concreți în ultima perioadă în direcția legii. Rămâne de văzut ce o să fie până în 2018. Sunt multe de discutat pe subiectul acesta. Norme și o grămadă de alte lucruri.

AGERPRES: Cum colaborați cu autoritățile statului pe partea de cybersecurity?

Dorin Pena: Avem o colaborare bună. Atâta vreme cât noi ne prezentăm tehnologiile noastre și cum pot tehnologiile noastre să ajute, oamenii sunt deschiși să înțeleagă și să aplice, în măsura în care se poate, la mediul fiecărei instituții.

AGERPRES: Aveți contracte cu instituții de stat?

Dorin Pena: N-aș putea să comentez lucrul acesta. Noi lucrăm prin intermediul partenerilor. Contracte directe în niciun caz și n-aș putea să comentez fără acordul unui client.

AGERPRES: La cel nivel se află România din punct de vedere al soluțiilor de securitate?

Dorin Pena: Este o analiză pe care nu am făcut-o și este destul de dificil să înțeleg la ce nivel. Sunt și aspecte bune și aspecte rele. Mă rog, să nu spunem rele, lucruri care pot fi îmbunătățite. Un lucru este cert. Dacă e să compar acum trei ani sau patru ani cu ce se întâmplă acum, am ajuns la un nivel mult mai ridicat de înțelegere a riscurilor și de cunoștințe ale oamenilor. Deficitul este destul de mare pe piața forței de muncă în ceea ce înseamnă specialiști calificați în securitatea cibernetică, dar măcar se înțeleg subiectul și importanța lui. Acum, spunea colegul meu de la Brinel, Marcel Borodi, că România este în topul atacurilor cibernetice. Aici trebuie înțeles, sunt multe lucruri de îmbunătățit și de aceea o reglementare pe securitate cibernetică pentru a stabili niște standarde clare este necesară.

AGERPRES: În afară de Directiva NIS, la nivel european este în discuție și o altă directivă — GDRP (General Data Protection Regulation). Termenul de implementare este tot 2018. În această privință s-au făcut pași?

Dorin Pena: Din câte știu, Directiva NIS este băgată sub Directiva GDRP. Dar, nefiind specialist în zona asta de legal și legislație UE, nu pot să spun cu certitudine acest lucru.

AGERPRES: Ați prezentat recent ultimul Raport Cisco de Securitate, cu date referitoare la securitatea cibernetică. Ați observat vreo schimbare în ultimii ani?

Dorin Pena: Da, am observat o schimbare de la nivelul de percepție a oamenilor până la nivelul de cunoștințe și, nu în ultimul rând, și la modalități de protecție. Piața de securitate, din punctul nostru de vedere — și avem și alte rapoarte — a fost în creștere în ultimii ani și noi considerăm că va fi în creștere în continuare, ne referim la piața de soluții de securitate, ceea ce spune că oamenii, companiile se preocupă de subiect, înțeleg subiectul, înțeleg gravitatea subiectului și, încet, încet, încep să ia măsuri.

AGERPRES: Totuși, oricât de bune ar fi soluțiile pe care le implementăm suntem vulnerabili...

Dorin Pena: Nu există o soluție care să te protejeze sută la sută. Aici este un joc pe cât de complicat, pe atât de simplu. Tot acest domeniu trebuie privit ca un business. La începuturile hacking-ului, mare parte din hacking era făcut de tineri specialiști în domeniul tehnologiei mai mult din instincte teribiliste. Hacking-ul a ajuns o industrie, este business. A fost evaluat în 2015 la 450 de miliarde de dolari la nivel mondial, cu o proiecție de 1.000 de miliarde de dolari în 2019 — 2020. O dublare într-un interval de cinci ani. Jocul este în a face task-ul, jobul hackerului cât mai greu și cât mai dificil, astfel încât să nu mai fie viabil din punct de vedere al resurselor, cost și timp. Și de aceea sunt toate metodele acestea. Este un lucru pe care noi l-am promovat de multă vreme și ne bucurăm să vedem că piața urmează trendul pe care Cisco oarecum l-a dat: este nevoie să gândim într-un mod integrat, într-o arhitectură. Nimănui nu i-ar plăcea să zboare cu un avion făcut din mai multe avioane. Trebuie lucrat integrat, astfel încât hackerul să fie nevoit să depună mult efort și mulți bani ca să găsească o vulnerabilitate și să treacă de toate sistemele de apărare pentru a ajunge la țintă.

AGERPRES: Tehnologiile avansează, la fel și atacurile. Cât ar putea dura cel mai rapid atac și cât de repede pot fi găsite soluțiile?

Dorin Pena: Am mai vorbit despre un atac la un resort de schi de lux din Austria, unde au fost blocate toate ușile și singura modalitate de deblocare a fost plătirea unei recompense. Acel atac a durat câteva secunde, dar în speță a existat o vulnerabilitate care a fost înțeleasă și exploatată de hackerii respectivi. Plaja este atât de largă și luni îți ia ca să faci o pregătire minuțioasă pentru a desfășura un atac în câteva secunde. Pe de altă parte, poți să infiltrezi lucruri pe care să le lași într-un proces de urmărire și le activezi în luni de zile, astfel încât să nu ți se identifice urma. Nu există un timp, de la câteva secunde la ani de zile pot dura atacurile cibernetice.

AGERPRES: Pe plan mondial, care a fost cel mai scump atac?

Dorin Pena: Nu știu exact... Din statisticile pe care le avem noi, costul mediu al unui atac este undeva la patru milioane dolari. 30% dintre companii recunosc că au pierdut clienți și 25% că au pierdut reputație. Recunosc, câți or mai fi dintre cei care nu recunosc. Aș da un exemplu de atac. La începutul acestui an a existat un atac de denial-of-service (DoS), adică blocarea furnizării unor servicii de către un service provider, un atac realizat la 10 milioane de dispozitive conectate la Internet, dintre care undeva peste 70% erau camere de luat vederi. Au fost compromise și au fost manipulate astfel încât să trimită o cantitate foarte mare de date și au distrus un serviciu care oferea rezolvarea numelui — se scrie www.x.ro și trebuie rezolvat în termeni IT — și o zonă importantă din SUA nu a mai funcționat din cauza acestei probleme, pentru că erau cei care ofereau serviciul acesta. Care au fost pagubele? Zeci de milioane.... Nici nu pot fi cuantificate.

AGERPRES: Puteți da exemple de atacuri mai deosebite din România?

Dorin Pena: Este destul de dificil să comentăm lucrurile care nu sunt publice, pentru că este nevoie de acordul clienților. Pentru noi contează foarte mult confidențialitatea și ajutăm clienții să-și remedieze problemele. Sunt două instituții ale statului român

specializate pe zona aceasta, CERT și Cyberint, și publică date destul de bine actualizate referitoare la statistici, la atacurile cibernetice din România. Ei sunt cei mai îndreptățiți să se pronunțe asupra situației.

AGERPRES: Atunci, care sunt sectoarele cele mai vulnerabile?

Dorin Pena: Din ceea ce vedem noi, nu suntem total diferiți de alte țări. Sunt foarte multe domenii care sunt atacate oarecum în mod egal, de la zona de utilități la zona de banking, în momentul în care un atac de tip ransomware îți poate bloca laptopul și, ca să ai acces la informații, trebuie să plătești, inclusiv zona de companii mici. Pentru că de la foarte multe companii mici dacă reușesc să iau o recompensă de 200-300 de dolari sau 500 de dolari, pentru a debloca fișierele contabile sau pozele... Și lumea plătește...

Și în ultima și în penultima formă a legii securității cibernetice se defineau niște tipuri de infrastructuri și se defineau niște obligații ale celor care operează anumite tipuri de infrastructuri și, ca exemplu, furnizorii de servicii de Internet aveau obligația ca într-un anumit timp să deconecteze, să informeze și să participe la remedierea unor probleme. Sunt lucruri pe care trebuie să le facem, pentru că o să vedeți, pierderile o să fie din ce în ce mai ... La ANAF sunt înregistrate vreo 400.000 de companii... dacă fiecare companie e atacată, să spunem, cu o medie de 100 de dolari, pe ransomware, target market-ul este la zeci de mii de dolari.

Lumea evoluează. Apropo de informații publice, citeam la un moment dat o analiză și concluzia era că anumite regimuri totalitare, cu toate metodele lor opresive, nu au reușit să strângă nicio mică parte din informațiile pe care noi în mod voluntar le facem publice.

AGERPRES: Cum ne putem apăra la nivel de persoană fizică, pe lângă soluțiile clasice? Și cui ne putem adresa în cazul în care cădem victimele unui astfel de atac?

Dorin Pena: Aici, din păcate, revenim la partea de reglementare. Nu există un cadru clar referitor la ce poate să facă un cetățean și de aceea se dorește și implementarea reglementării în securitate cibernetică și, potențial, să aibă și implicații de genul acesta. Eu aș simplifica-o cât de mult posibil. Primul lucru pe care ar trebui să-l facem ar fi să nu ne temem. Al doilea, ca să nu ne temem, să înțelegem că există un pericol și să-l acceptăm. Al treilea, să fim atenți la comportamentul nostru în web și în toată zona virtuală, pentru că internetul este relativ nou, la scara asta are 15 ani, e așa, la adolescență...Gândiți-vă, dacă e să comparăm cu viața unui om, cum o să fie la maturitate. Dar, de fapt, în această comparație, e abia la primele luni de viață... dar să revenim: să avem un comportament decent în zona asta, să fim atenți ce site-uri accesăm, ce link-uri clickăim, când primim e-mailuri de la cine le primim, ce fișiere descărcăm pe calculator sau pe telefon. Sunt reguli de bază, simple, pe care, în momentul în care le respectăm, scădem considerabil riscul de a fi infectați. Și... nu aveți la cine să apelați.

AGERPRES: Tot mai multe orașe sunt implicate în proiecte Smart City. La un moment dat aveați o colaborare cu Telekom pentru un astfel de proiect. Mai sunteți implicați și în altele?

Dorin Pena: Noi suntem furnizori de tehnologie și interacționăm cu o serie de parteneri. Într-adevăr, avem un pilot pe care l-am implementat cu Telekom, cu care avem un parteneriat mai mare la nivel de grupuri — Deutsche Telekom și Cisco — pentru Primăria sectorului 4. Acum, discuții referitoare la Smart City cred că sunt în ultimii patru ani foarte, foarte multe. Noi, de exemplu, am discutat concepte cu mai multe orașe, dar și cu Primăria sectorului 4. Știm din presă de Alba Iulia, știm și de Cluj, Constanța. Deci, cam toate orașele sunt interesate. Acum, nu tehnologia este cea mai importantă. Tehnologia este importantă, dar sunt și alte lucruri care trebuie stabilite atunci când vorbim de un oraș inteligent. Și trebuie plecat de la strategia clară pe care orașul o are pe o perioadă de câțiva ani. Nu pot să creez oraș inteligent în câteva luni, nu pot să creez oraș inteligent fără o alocare inteligentă a bugetelor. Și lucrurile astea trebuie puse într-un plan și, nu în ultimul rând, lucrul de care suferim, cel mai mult, execuția.

AGERPRES: Care este locul Cisco pe piața din România și ce cifră de afaceri a avut compania anul trecut?

Dorin Pena: Noi furnizăm soluții de tehnologii, de la partea de telecomunicații, securitate cibernetică, până la zona de centre de date sau service provideri, servicii și produse și software. Lucrăm cu tot felul de clienți. Acoperim, practic, toată plaja, de la clienți mari din sectorul public, până la clienți mici și mijlocii din zona de clienți privați. Cifra de afaceri nu putem să o spunem public, pentru că nu avem defalcat pe fiecare țară.

AGERPRES: Dar cum a evoluat în ultimii ani?

Dorin Pena: În ultimii ani, am avut un trend pozitiv, în trei ani și jumătate, pot să spun de când mă ocup eu.