**Mircea Bozga, Partener Risk Assurance, PwC România**

**Robert Girdoc, Senior Manager Risk Assurance, PwC România**

**Pierderile din cauza criminalității cibernetice depășesc cu mult investițiile în soluții de securitate. Companiile au înțeles riscurile și cresc fondurile alocate**

După provocările aduse de accelerarea digitalizării activității din timpul pandemiei, directorii generali din România încep să înțeleagă riscurile pe care această transformare le implică și au în plan creșterea investițiilor în securitatea cibernetică. Iar îngrijorările liderilor sunt cu siguranță legitime, ca răspuns la intensificarea atacurilor cibernetice din ultimii doi ani și în condițiile în care costul global al criminalității cibernetice aproape s-a dublat în 2020, comparativ cu 2018, situându-se la peste un trilion de dolari, potrivit unui raport realizat de compania americană de software antivirus McAfee.

Conștientizarea riscurilor și importanței unei strategii de securitate cibernetică a făcut un salt uriaș în timpul pandemiei, comparativ cu anii anteriori când companiile din România declarau că sunt la început de drum și când investiţiile în securitatea informatică erau impulsionate în principal de cerinţele de reglementare, după cum arăta un studiu realizat de PwC România și Microsoft în 2017. La vremea respectivă, 40% dintre companiile româneşti intervievate arătau că nu au o strategie de securitate informatică formal adoptată.

Reglementările rămân însă la fel de importante, mai ales în contextul obligativității de implementare a Legii 362/2018 (care transpune Directiva NIS - UE 2016/1148), prin care companiile care prestează servicii esențiale pentru populație trebuie să elaboreze și să implementeze soluții avansate care să le asigure securitatea informatică și protejarea infrastructurilor critice și să colaboreze cu statul pentru a garanta un răspuns coordonat la atacuri informatice. Sectoarele de activitate vizate sunt: energie (electricitate, petrol, gaze naturale), transport (aerian, feroviar, pe apă, rutier), sectorul bancar, infrastructuri ale pieței financiare, sectorul sănătății, furnizarea și distribuirea de apă potabilă și infrastructură digitală, dar și administrația publică.

**Directiva NIS, investiții necesare și rezultate**

Potrivit unui sondaj efectuat de ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) în noiembrie 2021, din aproape 1.000 de respondenți, 82% au implementat Directiva NIS, în timp ce 67% necesită buget suplimentar pentru a implementa toate cerințele acesteia.

Bugetul mediu alocat la nivelul statelor membre pentru implementarea directivei NIS a fost de 98.000 euro, România situându-se în a doua parte a clasamentului cu o sumă medie de 60.000 euro. Cele mai mari sume, între 100.000 și 140.000 euro, au fost alocate în Italia, Franța, Austria și Polonia, iar cele mai mici, de 20.000 euro, în Grecia, Malta și Letonia. Pe sectoare, cele mai multe fonduri au fost în sectorul energetic și cel bancar, iar cele mai mici în furnizarea și distribuția apei potabile, infrastructurile pieței financiare și infrastructura digitală.

De remarcat este faptul că sumele alocate pentru investiții sunt mult mai mici decât costurile directe ale unui incident major de securitate cibernetică estimate în medie la 169.000 euro, arată raportul ENISA -NIS Investments Report 2021. Iar rezultatele investițiilor deja se văd, aproape jumătate dintre respondenți, considerând că punerea în aplicare a directivei NIS le-a consolidat direct capacitățile de detectare a amenințărilor, iar 26% au raportat consolidarea capacităților de recuperare a datelor.

Nerespectarea implementării directivei NIS aduce după sine consecințe importante: de la sancțiuni din partea autorității competente la pierderi financiare în urma unor potențiale atacuri și chiar afectarea reputației.

**Atacurile cibernetice, locul cinci în topul amenințărilor la adresa companiilor din România**

Pe măsură ce organizațiile extind parteneriatele externe pentru a introduce noi soluții digitale și a le grefa pe propriile structuri IT, sistemele rezultate tind să genereze un risc cibernetic tot mai mare.

Iar acest lucru reiese și din cel mai recent sondaj global PwC ”Digital Trust Insights 2022”, potrivit căruia peste 60% dintre directorii generali și de tehnologie anticipează o creștere a criminalității cibernetice și în 2022, în fruntea listei țintelor pentru atacuri aflându-se rețelele mobile, Internet of Things (IoT) și serviciile cloud.

Aproape 60% dintre respondenți se așteaptă la o creștere a atacurilor asupra serviciilor lor de cloud, iar 56% prevăd mai multe breșe de securitate la nivelul furnizorilor lor de software. În același timp, respondenții estimează o creștere semnificativă a atacurilor ransomware.

În România, atacurile cibernetice se află pe locul cinci în topul amenințărilor la adresa perspectivelor de dezvoltare a companiilor, arată sondajul CEO Survey România 2021, astfel că, dacă în trecut securitatea informatică era o problemă doar a departamentului IT, în acest moment a devenit o prioritate pe agenda directorilor generali, necesitând o abordare strategică și reprezentând o responsabilitate a întregii organizații. Dincolo de supraveghere și protecție din punct de vedere tehnic în fața pericolelor, eforturile de securitate trebuie să se concentreze și pe inițiative de digitalizare a modelelor de business, eco sistemelor și proceselor interne.

Și, din moment ce digitalizarea va continua, marea majoritate (85%) a directorilor generali din România planificând majorări ale investițiilor în transformarea digitală, în următorii trei ani, ei vor crește și fondurile pentru securitatea cibernetică. Peste o treime (35%) au spus că investițiile lor în acest domeniu vor crește semnificativ, cu 10% sau mai mult.

România se înscrie astfel mai degrabă în trendul global, decât cel regional. Potrivit CEO Survey, directorii generali de la nivelul Europei Centrale și de Est plasează atacurile cibernetice abia pe locul zece în topul amenințărilor și numai 27% vor crește investițiile cu peste 10% în acest domeniu. În schimb, la nivel global creșterea semnificativă a numărului incidentelor de securitate cibernetică din 2020 a propulsat amenințările cibernetice pe locul doi în topul preocupărilor, imediat după pandemii, iar 31% dintre directorii globali au în plan creșterea investițiilor cu două procente.