Una din cinci organizatii a ajuns în pragul insolventei dupa un atac cibernetic

Una din cinci organizatii a ajuns în pragul insolventei dupa un atac cibernetic, potrivit unui articol postat pe Eset Blog, unde se atrage atentia ca atacurile cibernetice sunt o amenintare cât se poate de reala pentru organizatii.

"Ştim cu totii ca securitatea cibernetica este un element critic de risc pentru afaceri. Dar cât de critic? Desi unele companii au o atitudine mai relaxata asupra acestui aspect si nu asigura un suport real acestei componente, acestea reusesc chiar si în aceste conditii sa evite repercusiuni grave. Un nou raport al asiguratorului global Hiscox face însa obiectul unei lecturi interesante. Acesta sustine ca multe organizatii europene si americane au fost la un prag de insolventa dupa ce au suferit brese de securitate. Şi, desi investitiile companiilor în ceea ce priveste securitatea informatica a infrastructurii sunt în crestere, la nivel global, mai putine companii ca niciodata pot fi descrise ca fiind 'experte' în pregatirea cibernetica", se spune în articol.

Identificarea locului anume unde sa directionezi investitiile în securitatea IT nu a fost niciodata mai importanta. Iar un amestec între implementarea celor mai bune practici si disponibilitatea companiilor de a învata din incidentele anterioare suferite este, potrivit raportului, solutia pentru a evita falimentul.

Raportul este întocmit în urma unor interviuri cu 5.000 de companii din SUA, Marea Britanie, Belgia, Franta, Germania, Spania, Olanda si Irlanda. Unele dintre constatari se cunosteau deja, însa exista si alte câteva nuante interesante în acest raport, cum ar fi: sapte din opt tari considera atacul cibernetic drept principala amenintare la adresa afacerii lor; jumatate (48%) dintre respondenti au raportat un atac cibernetic în ultimele 12 luni, în crestere fata de 43% anul trecut; o cincime (19%) dintre respondenti au raportat un atac ransomware, în crestere de la 16%; doua treimi dintre victime au platit rascumpararea în urma atacurilor.

"Nimic neobisnuit pâna acum. Cu toate acestea, exista o mare prapastie în perceptie între cei care au suferit deja un atac cibernetic si cei care nu au trecut printr-un astfel de incident. Mai mult de jumatate (55%) dintre victimele atacurilor informatice considera securitatea cibernetica o zona cu risc ridicat, dar cifra scade la doar 36% pentru cei care nu au experimentat înca un atac de compromitere de date. În mod similar, 41% dintre cei atacati spun ca expunerea lor la risc a crescut, dar pentru celalalt grup cifra este mai mica de un sfert (23%)", sustin specialistii Eset.

Un alt element interesant din acest raport este faptul ca infractorii cibernetici par sa vizeze din ce în ce mai mult companiile mai mici. Astfel ca cei cu venituri de 100.000 de dolari - 500.000 de dolari se pot astepta acum la tot la fel de multe atacuri, similar celor care au o cifra de afaceri între 1 si 9 milioane dolari anual.

Foarte important este ca o cincime dintre firmele respondente care au fost atacate spun ca solvabilitatea lor a fost amenintata, o crestere cu 24% fata de anul trecut. Desi nu sunt dezvaluite în raport, costurile breselor de securitate pot presupune: întreruperi operationale, costurile legale, orele suplimentare IT si costurile pentru firme terte de investigatie si remediere, amenzi de reglementare, pierderea clientilor, pierderea productiei si a vânzarilor, daune reputationale pe termen lung. Aceasta poate fi o explicatie partiala pentru cresterea cheltuielilor.

Bugetele medii pentru securitatea cibernetica ale respondentilor au crescut cu 60% în ultimul an, ajungând la suma de 5,3 milioane dolari, si cu 250% fata de 2019, potrivit raportului.

Potrivit raportului, principalii vectori de atac sunt: serverele cloud (41%), e-mailurile business (40%), serverele corporative (37%), serverele cu acces de la distanta (31%), dispozitivele mobile detinute de angajati (29%), DDoS - distributed denial-of-service (26%).

"Acest lucru este în acord cu constatarile altor rapoarte si cu relatarea conform careia munca de la distanta, investitiile din timpul pandemiei în infrastructura cloud si provocarile de securitate datorate sistemul de tip work-from-home sunt unele dintre cele mai mari riscuri cu care se confrunta organizatiile în prezent. Acestea, combinate cu eroarea umana, au dus la extinderea suprafetei de atac pe care o pot tinti acum actorii amenintarilor", precizeaza specialistii Eset.

O oarecare îngrijorare genereaza faptul ca scorurile de pregatire cibernetica ale companiilor estimate de Hiscox au scazut cu 2,6% de la an la an, ceea ce a condus la o scadere brusca a numarului de firme clasate drept "experte" - de la 20% la doar 4,5%. Proportia companiilor clasate ca începatoare a scazut de asemenea semnificativ, astfel ca majoritatea firmelor au fost desemnate ca "intermediare". Pregatirea cibernetica conteaza, dupa cum se poate demonstra, costurile medii ale atacurilor ca procent din venituri fiind de doua ori si jumatate mai mari pentru firmele clasificate drept "novice cibernetic", sustine raportul.

Expertii Eset recomanda companiilor: sa formalizeze securitatea cibernetica din companie, cu roluri clar definite, implicând totodata consiliul director sau managerii seniori; sa se asigure ca directorii de top au vizibilitate clara si implicare în procesele de securitate cibernetica, sa urmeze standardele de bune practici, cum ar fi cadrul oferit de Institutului National de Standarde si Tehnologie din SUA (NIST), sa împarta investitiile între toate cele cinci functii cheie ale NIST - identificare, protectie, detectie, raspuns la incident si recuperare, sa se concentreze pe planificarea raspunsului la incident si pe simulari de atac, mai ales în contextul incertitudinii geopolitice actuale, sa evalueze în mod regulat infrastructura de stocare date si de tehnologie corporativa, sa ofere angajatilor cursuri eficiente de constientizare a securitatii cibernetice, sa se asigure ca furnizorii si partenerii de afaceri respecta cerintele de securitate, sa se concentreze pe procese cu rezultate imediate, precum patching, pentesting si backup-uri regulate.

"Toti acesti pasi cumulati vor ajuta la minimizarea sanselor ca businessul sa ajunga la faliment în urma unui atac cibernetic", dau acestia asigurari.