BUSINESS SOS

GHID CYBER RISK

INFORMAȚII UTILE PENTRU ANTREPRENORI

CONSIDERI CĂ AI LUAT TOATE MĂSURILE NECESARE CA AFACEREA TA SĂ NU FIE ȚINTA UNUI ATAC CIBERNETIC? CREZI CĂ AFACEREA TA ESTE SUFICIENT DE PROTEJATĂ ÎN FAȚA ATACURILOR CIBERNETICE?

ÎN CAZUL ÎN CARE NU EȘTI SIGUR DE RĂSPUNSURILE LA ÎNTREBĂRILE DE MAI SUS, ÎȚI RECOMANDĂM SĂ INVESTEȘTI ÎN INFORMAȚIE PENTRU A LUA CELE MAI BUNE DECIZII PENTRU VIITORUL BUSINESS-ULUI TĂU.

Un demers inițiat de:

UNSAR 27 DE ANI

www.asiguropedia.ro

Powered by

ASIGUROPEDIA

Asigură-te că știi!

Securitatea cibernetică reprezintă una dintre principalele provocări cu care ne confruntăm în ultima perioadă. Totodată, este și una dintre principalele îngrijorări ale românilor, aproape jumătate dintre aceștia spunând că este probabil și foarte probabil să fie ținta unui atac cibernetic, arată un studiu sociologic realizat de IRES, la solicitarea UNSAR, anul trecut.

Cu cât o societate este mai dezvoltată din punct de vedere al tehnologiei informației, cu atât este mai vulnerabilă în fața diverselor tipuri de atacuri, iar asigurarea spațiului cibernetic trebuie să constituie principala preocupare a tuturor actorilor implicați.

CE ESTE RISCUL CIBERNETIC?

Riscul cibernetic poate fi definit ca fiind orice risc care decurge din utilizarea tehnologiei informațiilor și a comunicațiilor (conform Geneva Association). Riscurile cibernetice reprezintă o amenințare reală și capătă dimensiuni importante de la an la an. Atacurile cibernetice și criminalitatea informatică sunt tot mai numeroase și mai sofisticate în întreaga Europă. Se estimează că la nivel mondial 22,3 miliarde de dispozitive vor fi conectate la Internetul Lucrurilor până în 2024, conform datelor Comisiei Europene.

CE ESTE ATACUL CIBERNETIC?

Acesta poate fi definit ca fiind orice acțiune ostilă desfășurată în spațiul cibernetic de natură să afecteze confidențialitatea, integritatea, disponibilitatea, autenticitatea informațiilor în format electronic, a resurselor și serviciilor publice sau private din spațiul cibernetic (securitatea cibernetică) .

CARE POATE FI IMPACTUL UNUI ATAC CIBERNETIC ASUPRA UNEI AFACERI?

În funcție de prejudiciile produse, impactul unui atac cibernetic poate duce la întreruperea afacerii, pierderea proprietății intelectuale, pierderea reputației, a cotei de piață, pierderi bănești, încălcare a legii care va genera amenzi și alte costuri adiționale.

CARE SUNT CELE MAI IMPORTANTE ACTIVITĂȚI DE TIPUL AMENINȚĂRILOR CIBERNETICE CARE POT PREJUDICIA ACTIVITATEA UNEI AFACERI?

Conform raportului publicat de Agenția Uniunii Europene pentru Securitate Cibernetică – ENISA în octombrie 2020, topul amenințărilor cibernetice în perioada 2019-2020 a fost reprezentat de "programe malware" (software dezvoltat pentru a dobândi accesul la un dispozitiv sau a-i aduce daune fără ca deținătorul să își dea seama, utilizat și în activitățile de spionaj), atacuri prin internet, phishing (acțiuni frauduloase privind furtul datelor utilizatorilor, datelor de conectare sau diverse informații referitoare la cardurile de credit, prin deghizare sub formă de sursă credibilă) și, nu în ultimul rând, de activitatea de spam (transmiterea de mesaje nesolicitate în grup, ca mijloc de distribuire sau de facilitare a altor amenințări).

Conform definiției din Strategia de securitate cibernetică a României.

Și la nivel național aceste atacuri cibernetice capătă noi cote importante, iar prin intermediul Centrului Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO se transmit alerte privind anumite vulnerabilități sau chiar atacuri cibernetice de impact.

CONFORM THE **GLOBAL RISKS REPORT 2021**, EȘECUL SECURITĂȚII CIBERNETICE SE AFLĂ PRINTRE CELE MAI PROBABILE RISCURI CARE VOR DOMINA ÎN URMĂTORII 10 ANI.

CUM MĂ POT PROTEJA ÎMPOTRIVA UNUI ATAC CIBERNETIC?

Există mai multe măsuri pe care le poți lua pentru a te proteja împotriva unor atacuri cibernetice.
Dacă ești interesat de un ghid de bune practici pentru securitate cibernetică, îl poți vizualiza AICI pe cel publicat de Serviciul Român de Informații.
De asemenea, CERT-RO a publicat anul trecut un infografic care conține 5 sfaturi pentru angajați pentru a preveni fraudarea companiei tale, pe care îl poți vizualiza AICI.
Totodată, o altă măsură de siguranță în care poți investi este asigurarea pentru riscuri cibernetice care reprezintă un instrument care poate completa planul de gestionare a incidentelor de securitate cibernetică, incidente la care poate fi expus business-ul la un moment dat.

CE ESTE ASIGURAREA PENTRU RISCURI CIBERNETICE?

Asigurarea pentru riscuri cibernetice reprezintă o soluție de protecție împotriva pierderilor financiare - de care poți beneficia în cazul incidentelor de securitate legate de date și informații sensibile. Aceste asigurări sunt customizabile și pot acoperi atât daunele proprii, cât și daunele produse terților (partenerilor de business) cauzate de un atac cibernetic produs asupra companiei tale.

ACESTE ASIGURĂRI SUNT DISPONIBILE PENTRU ORICE TIP DE ACTIVITATE DESFĂȘURAT DE COMPANIE?

În general, reprezintă o soluție viabilă pentru categoriile de business care gestionează cantități mari de date.
Prin urmare, este o soluție potrivită și pentru tine dacă activezi în domenii precum cel financiar, IT, medical, transporturi, e-commerce, turism și recreere, companii de utilități, telecomunicații etc.

CARE SUNT RISCURILE PE CARE LE POATE ACOPERI O ASIGURARE ÎMPOTRIVA ATACURILOR CIBERNETICE?

Principalele riscuri care pot fi acoperite printr-o astfel de asigurare sunt: pierderi sau deteriorări ale datelor și sistemelor, pierderi de profit ca urmare a întreruperii activității (cauzată de un atac cibernetic) – inclusiv costurile suplimentare necesare pentru reluarea activității, răspunderea companiei pentru datele colectate, utilizate și stocate, de la clienți/parteneri/angajați, riscuri reputaționale, cheltuieli generate în procesul de apărare în instanță, amenzi și penalități ale autorităților etc. În funcție de specificul activității tale, îți poți personaliza acoperirile pe acest tip de asigurare, și îți recomandăm să contactezi distribuitorul tău în asigurări specializat în riscuri cibernetice pentru a putea beneficia de consultanța necesară în luarea celei mai bune decizii privind protejarea business-ului tău și identificarea produselor care corespund cel mai bine cerințelor și necesităților tale.

PENTRU CE PERIOADĂ POT ACHIZIȚIONA ACEASTĂ ASIGURARE?

În general, aceasta are o valabilitate de 12 luni, timp în care poți beneficia de acoperire pentru eventuale prejudicii pe care le-ai suportat în urma unui atac cibernetic. În anumite condiții ai putea beneficia de o perioadă de anterioritate – adică poți fi acoperit și pentru anumite incidente cibernetice produse în perioada de dinaintea începerii perioadei asigurate menționate în polița de asigurare. De asemenea, se poate include și o perioadă de raportare extinsă – care îți permite avizarea incidentelor cibernetice petrecute în perioada asigurată până într-un anumit interval de timp de la expirarea poliței de asigurare.

71%

DINTRE COMPANII ȘI ORGANIZAȚII S-AU CONFRUNTAT CU AMENINȚAREA DE TIPUL PROGRAMELOR MALWARE.

Sursa: https://www.consilium.europa.eu/ro/infographics/cybersecurity-in-the-eu/

ASUPRA CĂROR ASPECTE AR TREBUI SĂ ACORD O IMPORTANȚĂ SPORITĂ ÎNAINTE DE ÎNCHEIEREA UNEI ASIGURĂRI ÎMPOTRIVA ATACURILOR CIBERNETICE?

Este foarte important să știi că, înainte de încheierea oricărei polițe, inclusiv de acest tip, distribuitorul are obligația legală ca, într-o primă etapă să îți pună la dispoziție informații cu caracter general despre această asigurare sub forma unui document standardizat denumit - PID. Informațiile trebuie să se refere cel puțin la: riscurile acoperite, suma sau sumele asigurate (sau limitele de răspundere) la care s-ar putea încheia asigurarea, riscurile excluse pentru care nu se acordă despăgubiri, metode de plată a primelor și frecvența plăților, obligațiile care revin asiguratului în baza contractului, inclusiv când se solicită despăgubiri, durata contractului și metodele de încetare a acestuia.
A doua etapă obligatorie pe care trebuie să o parcurgă un distribuitor constă în acordarea de consultanță, înainte de emiterea unei asigurari.

66%

DINTRE AMENINȚĂRILE CIBERNETICE LEGATE DE PANDEMIA COVID-19 PROVIN DIN E-MAILURILE SPAM.

Sursa: https://www.consilium.europa.eu/ro/infographics/cybersecurity-in-the-eu/

AI INVESTIT PREA MULT ÎN BUSINESS-UL TĂU CA SĂ NU ÎL PROTEJEZI!

- Costul mediu al unei încălcări a datelor este de 3,86 milioane de dolari începând cu 2020.
- Timpul mediu pentru identificarea unei încălcări a datelor în 2020 a fost de 207 de zile.
- Datele cu caracter personal au fost implicate în 58% din încălcări în 2020.

Sursa: https://www.varonis.com/blog/cybersecurity-statistics/

PIERDERILE FINANCIARE LA NIVEL GLOBAL ESTIMATE PENTRU 2021 CA URMARE A UNOR RISCURI CYBER

6 trilioane $ de dolari pe an
500 miliarde $ pe lună
115.4 miliarde $ pe săptămână
16.4 miliarde $ pe zi

684.9 milioane $ pe oră
11.4 milioane $ pe minut
190.000 $ pe secundă

Sursa: Cybersecurity Ventures

ÎNTR-O SINGURĂ LUNĂ DIN TIMPUL PANDEMIEI DE COVID-19 S-A OBSERVAT O CREȘTERE CU

+667%

A INȘELĂTORIILOR PRIN PHISHING.

Sursa: https://www.consilium.europa.eu/ro/infographics/cybersecurity-in-the-eu/

ÎN CE CONSTĂ CONSULTANȚA ȘI DE CE ESTE IMPORTANT SĂ BENEFICIEZ DE CONSULTANȚĂ DIN PARTEA DISTRIBUITORULUI DE ASIGURĂRI?

În cadrul acestei etape, distribuitorul evaluează, în primul rând, cerințele și necesitățile concrete pentru care intenționezi să închei o poliță de asigurare împotriva riscurilor cibernetice, evaluare care se realizează în baza unui document (chestionar) denumit DNT care îți este pus la dispoziție de către distribuitor și pe care trebuie să-l completezi. În urma acestei etape, distribuitorul va putea genera o ofertă de asigurare personalizată.
În acest fel vei putea lua o decizie asumată cu privire la o soluție care să-ți ofere sprijinul financiar necesar continuității afacerii în cazul unui atac cibernetic.