BUSINESS SOS

GHID RISCURI CIBERNETICE

INFORMAȚII UTILE PENTRU ANTREPRENORI

Niciun antreprenor nu concepe dezvoltarea afacerii sale în absența instrumentelor digitale. Dar beneficiile vin și cu riscuri ... cibernetice. Ai luat în calcul să-ți protejezi afacerea de un eventual atac cibernetic? Ai întrebări? Iată raspunsurile!

Un demers inițiat de

UNSAR 28 DE ANI

www.asiguropedia.ro

Powered by

ASIGUROPEDIA
Asigură-te că știi!

Pandemia a obligat business-urile să accelereze procesul de digitalizare. În afară de beneficiile evidente, digitalizarea vine și cu riscuri:

32% dintre români au indicat un interes mai ridicat de a se proteja în fața riscurilor cibernetice de tipul furt de date de pe card, parole etc. (Barometrul UNSAR-IRES despre "Percepția riscului și cultura asigurărilor din România", 2021).

Conform unui alt studiu, aproape **jumătate dintre români au spus în 2021 că este probabil și foarte probabil să fie ținta unui atac cibernetic.**

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).

Avansul tehnologic sau digitalizarea fac acum parte din viața noastră, și aduc cu sine riscuri specifice. De la 400 de atacuri cibernetice pe minut în 2021, acum sunt înregistrare 550 de asemenea atacuri pe minut, conform datelor Bitdefender.

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 AMENINȚĂRI CIBERNETICE CARE POT PREJUDICIA ACTIVITATEA UNEI AFACERI?

Conform raportului publicat de Agenția Uniunii Europene pentru Securitate Cibernetică – ENISA în octombrie 2021, topul amenințărilor cibernetice în perioada 2020-2021 a fost reprezentat de:

RANSOMWARE - un software rău intenționat care, după ce se instalează pe dispozitivul victimei, criptează datele victimei ținându-le „ostatice” sau șantajează victima, pe care o amenință că îi va publica datele dacă aceasta nu plătește o „răscumpărare”

MALWARE - software dezvoltat pentru a dobândi accesul la un dispozitiv sau a-i aduce daune fără ca deținătorul sa își dea seama, utilizat și în activitățile de spionaj

CRYPTOJACKING - actul de deturnare a unui computer pentru a extrage criptomonede împotriva voinței utilizatorilor, prin intermediul site-urilor web sau în timp ce utilizatorul nu este conștient

SPAM ȘI ATACURI PRIN INTERMEDIUL E-MAILULUI - transmiterea de mesaje nesolicitate în grup, ca mijloc de distribuire sau de facilitare a altor amenințări

ATACURI ÎMPOTRIVA SECURITĂȚII DATELOR

Și la nivel național aceste atacuri cibernetice capătă o nouă amploare. Prin intermediul Directoratului Național de Securitate Cibernetică - DNSC se transmit alerte privind anumite vulnerabilități sau chiar atacuri cibernetice de impact.

CUM TE POȚI PROTEJA ÎMPOTRIVA UNUI ATAC CIBERNETIC?

Există mai multe măsuri pe care le poți lua pentru a te proteja împotriva unor atacuri cibernetice.

Asigurarea pentru riscuri cibernetice este un instrument ce poate completa planul de gestionare a incidentelor de securitate cibernetică la care poate fi expus business-ul la un moment dat.

Daca 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, DNSC a publicat un infografic care conține 5 sfaturi pentru angajați pentru a preveni fraudarea companiei tale, pe care îl poți vizualiza **AICI**.

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 pot fi personalizate și pot acoperi atât daunele proprii, cât și daunele produse terților (partenerilor de business) cauzate de un atac cibernetic produs asupra companiei tale.

CE TIP DE ACTIVITATE TREBUIE ASIGURATĂ?

În general, aceste polite sunt o soluție viabilă pentru categoriile de business care gestionează date personale sau informații confidențiale (de exemplu, informații comerciale) sau care utilizează tehnologie informatică (calculatoare, servere, conexiune la internet).

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.

În primele 3 luni ale anului 2022 au fost înregistrate 431 infracțiuni contra siguranței și integrității sistemelor și datelor informatice și 2719 fraude comise prin sisteme informatice și mijloace de plată electronice, conform datelor publicate de Poliția Română.

CE TREBUIE SĂ ȘTII CÂND ÎNCHEI O ASIGURARE ÎMPOTRIVA RISCURILOR 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 asigurări.

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

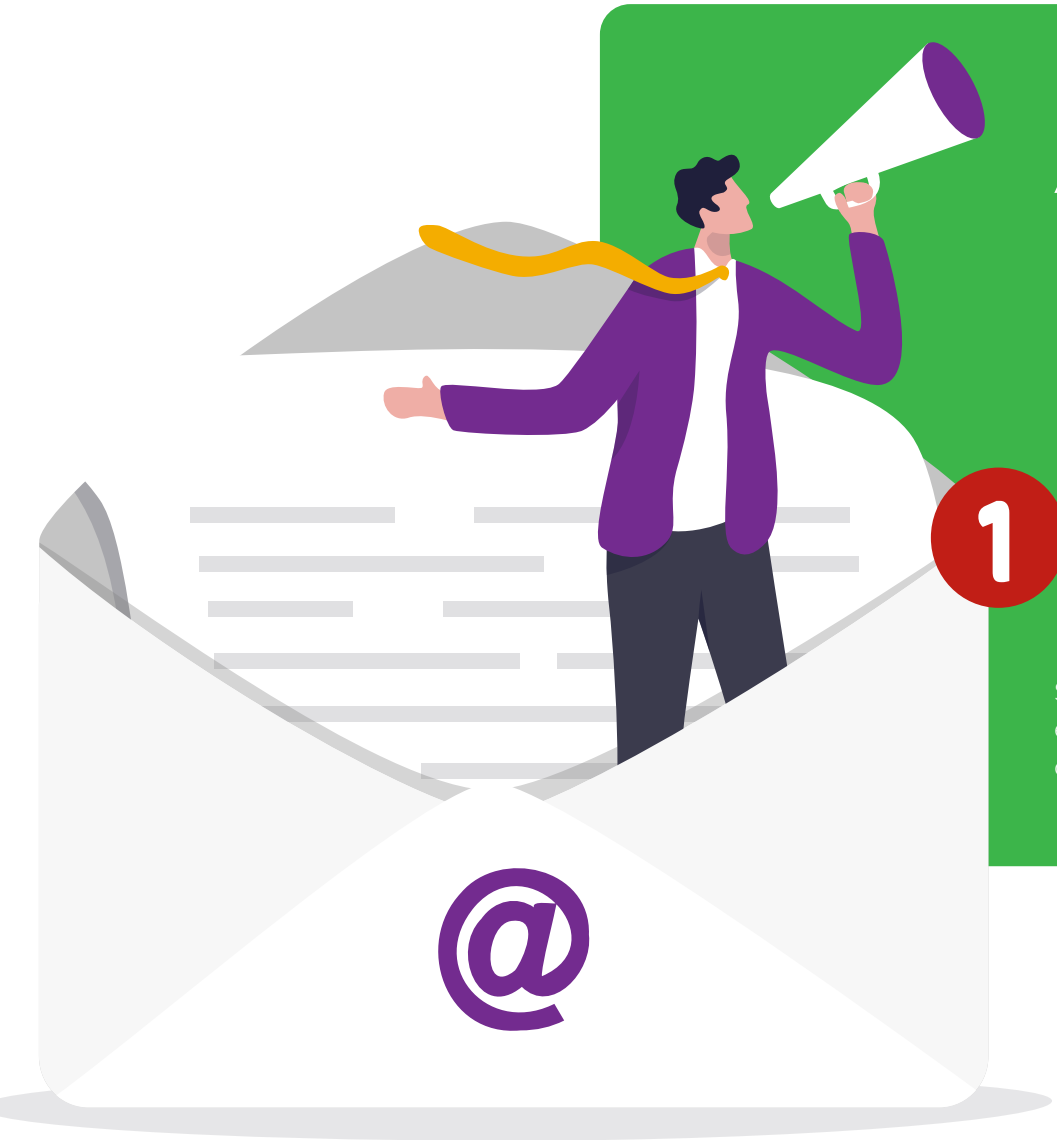
În cadrul acestei etape, distribuitorul evaluează, în primul rând, cerințele și necesitățile concrete pentru care intenționezi să închei o poliță de asigurare împotriva riscurilor cibernetice, care se realizează în baza unui document (chestionar) denumit DNT, pus la dispoziție de către distribuitor și 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-și ofere sprijinul financiar necesar continuității afacerii în cazul unui atac cibernetic.

CARE SUNT CONSECINȚELE FINANCIARE ALE RISCURILOR CIBERNETICE?

* Daunele cauzate de criminalitatea cibernetică globală vor atinge 10,5 trilioane de dolari anual până în 2025.
* Cheltuielile globale pentru asigurarea securității cibernetice vor depăși 1,75 trilioane de dolari cumulat în perioada 2021-2025.
* Se estimează că costurile globale ale daunelor cauzate de atacuri de tip ransomware vor depăși 265 de miliarde de dolari până în 2031.
* Lumea întreagă va trebui să asigure protecție cibernetică pentru 200 zettabytes de date până în 2025.
* Se estimează că piața globală a asigurărilor cibernetice va atinge 14,8 miliarde de dolari anual până în 2025.

Sursa: Cybersecurity Ventures



66% DINTRE AMENINȚĂRILE CIBERNETICE LEGATE DE PANDEMIA COVID-19

1 PROVIN DIN E-MAILURILE SPAM.

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

Nu îți asuma riscuri inutile! Planul Business SOS, promovat de UNSAR, este sprijinul de care ai nevoie pentru a găsi informatii relevante despre asigurările de bunuri, răspunderi civile, asigurări pentru riscuri financiare și, nu în ultimul rând, despre asigurările împotriva riscurilor cibernetice.