Ciberseguretat, com protegir els sistemes de la seva empresa

Malware, injecció de codi SQL, phishing, 'Man in the middle' o atac de denegació de servei són alguns dels mètodes més comuns per amenaçar la ciberseguretat de les empreses. A aquests cal sumar-los els possibles errors que els usuaris poden cometre usant els sistemes informàtics i les polítiques de seguretat laxes que permeten l'accés no autoritzat a informació confidencial. En els últims anys, atacs i descuits com aquests es repeteixen posant en dubte les infraestructures i la informació de les organitzacions.

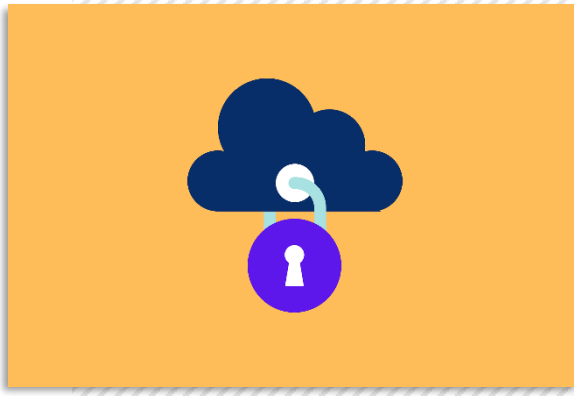
Risk Based Security, l'agència internacional d'intel·ligència de vulnerabilitats, filtració de dades i qualificacions de risc, va publicar un informe en què va confirmar que durant els 9 primers mesos de 2019 es va produir la filtració d'uns 7.900 milions de registres, fet que suposa un 112% més que el 2018. I que el 2020 aquesta xifra es va incrementar malgrat el recés inicial provocat per la situació excepcional de pandèmia. Els àmbits més afectats van ser els serveis mèdics, els minoristes i les entitats públiques.

Aquestes dades posen de manifest la necessitat, per part de les empreses, de disposar d'un **protocol de ciberseguretat** o un **pla de seguretat informàtica** perquè puguin protegir equipament, persones i dades de possibles atacs maliciosos. No només pel fet de treballar amb ordinadors i xarxes, sinó perquè cada vegada més s'incorporen nous elements de comunicació (dispositius mòbils, sistemes electrònics, servidors al núvol, etc.) que poden ser vulnerables a amenaces externes si no es disposa d'una política de protecció dels mateixos.

Hi ha estàndards, mètodes i eines per minimitzar els possibles riscos als quals s'enfronten les companyies. **L'Institut Nacional de Ciberseguretat, INCIBE**, facilita a totes les pimes multitud de recursos perquè puguin posar en marxa i executar protocols de protecció en diferents àrees amb l'objectiu d'identificar i eliminar vulnerabilitats. Apuntem a continuació, algunes idees basades en la nostra experiència, que ens ajuden a definir conceptes i impulsar línies estratègiques per al nostre negoci.

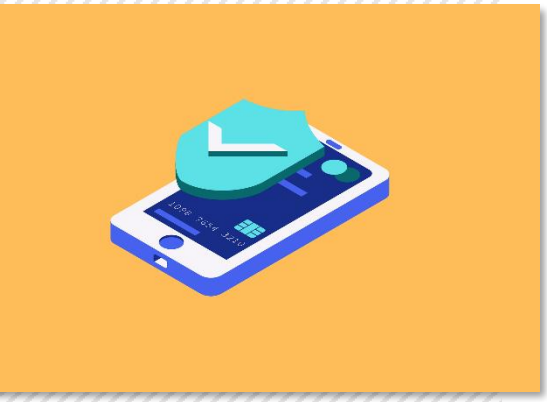
Els principals actius que són susceptibles de patir ciberamenaces i que hem de cuidar són la infraestructura, els usuaris i la informació. Basant-nos en ells podem establir diferents categories en l'àmbit de seguretat:

- Seguretat de xarxa.
- Seguretat de les aplicacions (començant en l'etapa de disseny).
- Seguretat de la informació.
- Seguretat operativa (permisos d'usuari i emmagatzematge de dades).
- Recuperació davant agents externs.
- Capacitació de l'usuari final.



Per garantir la integritat de la nostra empresa i complir amb el nivell de protecció desitjat, cal definir i executar un pla de seguretat. Aquest **pla de seguretat** ha de ser l'element director dels protocols, les accions i les tècniques indispensables per a protegir l'organització de possibles ciberamenaces. L'objectiu és ser proactius i anticipar-se als possibles atacs.

Comencem el pla de seguretat amb una anàlisi de **riscos informàtics**. Hem d'identificar els diferents actius, les seves vulnerabilitats i amenaces i la probabilitat que aquestes es produeixin. D'aquesta manera podrem establir accions concretes per evitar els danys que causarien l'existència i propagació d'un risc a la nostra xarxa. Caldrà, doncs, la creació d'una arquitectura de seguretat que preservi la confidencialitat, la integritat i la disponibilitat dels recursos susceptibles de ser atacats i la privacitat de les dades. Acabem aquesta fase documentant tot el procediment en una **matriu de risc**.



Avançant en el nostre **pla de seguretat**, elaborarem processos específics per a cada servei, definirem accions i persones responsables i proporcionarem els recursos i drets d'accés coherents per a cada usuari. Un cop més, el monitoratge continu i en temps real de tots els recursos ens ajudarà a detectar de forma ràpida qualsevol intrusió o acció negativa cap al nostre sistema. En aquest sentit podem usar sistemes de detecció d'intrusions (IDS), eines de gestió d'informació i incidències (SIEM) i solucions de seguretat de resposta automatitzada (SOAR). A més, és important i necessari que els empleats estiguin alineats amb la política de seguretat de la companyia, per a això serà indispensable formar-los i conscienciar-los. A continuació, llistem una sèrie de mesures que considerem essencials per assegurar un sistema estàndard:

- Tècniques de desenvolupament per al programari (ISO 27001).
- Ús de maquinari fiable amb sistema de connexió per a accés i informació encriptada amb TPM 2.0.
- Sistemes d'informació actualitzats.
- Accés a la infraestructura de sistema controlat amb mesures físiques: sistemes antiincendis, proteccions elèctriques, etc.
- Encriptació i xifrat de la informació.
- Contrasenyes complexes.
- Doble autenticació per als usuaris.
- Autenticació mitjançant certificats SSL dels dispositius que es connecten a les nostres xarxes.
- Vigilància de xarxa, especialment en les sense fils.
- Xarxes perimetrals de seguretat.
- Tecnologies protectores: tallafocs, antispyware, antivirus, etc.
- Còpies de seguretat i sistemes de suport remot d'informació (backups).
- Control de l'accés a la informació.
- Recopilació i anàlisi d'informació de seguretat.
- Protecció de dispositius amb solucions EDR.

El **pla de seguretat** de la nostra empresa ha de ser un document viu i revisable per anar incorporant totes les novetats en matèria de ciberseguretat i els nous processos i eines de l'empresa. La implicació dels equips directius serà un element clau perquè aquesta política es consolidi en l'organització.

Apostar seriosament per la seguretat és una virtut diferencial, especialment, per a les companyies creadores de programari. Avui dia és indispensable garantir que la identitat dels productors de solucions informàtiques estables, eficaces i segures, destil·la els valors que difon. A major grau d'innovació en els serveis, millors protocols de seguretat que refermen equips, dispositius, informació i l'activitat de les persones per, a la fi, generar llaços estrets de confiança entre clients i usuaris.