OFICINA Acelera pyme

Diputació de Girona

CONSELL COMARCAL DE L'ALT EMPORDÀ

España | digital 2026

Com evitar el robatori de dades en el vostre negoci

Ayub Nakmoussi Harrak – BDR Informàtica

10 de març de 2023 – (Ca l'Anita) Roses

Finançat per la Unió Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

Pla de Recuperació, Transformació i Resiliència

1. Definició de ciberseguretat i importància per a les empreses i comerços
    - 1.1 Definició de ciberseguretat
    - 1.2 Impacte dels ciberatacs
    - 1.3 Qui hi ha al darrere el cibercrim?
2. A què s'enfronten les empreses i els comerços actualment?
3. Com entren aquestes amenaces en els nostres sistemes informàtics?
4. 10 consells per a mantenir-nos ciberprotegits a l'empresa o la nostra botiga
5. Política de seguretat informàtica
6. Conclusió

1. Definició de ciberseguretat i importància per a les empreses i comerços

1.1 Definició de ciberseguretat

QUÈ ÉS LA CIBERSEGURETAT?

La ciberseguretat engloba el conjunt de mesures físiques, lògiques i administratives destinades a la protecció digital de les empreses, persones i sistemes (siguin dispositius, aplicacions o dades) davant d'atacs digitals que puguin comprometre'n la confidencialitat, disponibilitat o integritat

1. Definició de ciberseguretat i importància per a les empreses i comerços

1.1 Definició de ciberseguretat

EN QUÈ CONSISTEIX?

Els sistemes ciberfísics equipats amb la tecnologia d'Internet **requereixen conceptes i tecnologies fiables per a garantir la seguretat, la privacitat i la protecció del coneixement** Per tant, és crucial **comptar amb unes comunicacions fiables i segures** juntament amb una identitat sofisticada i una gestió de l 'accés de les màquines.

Sobre aquests actius, **es defineixen i s'implementen diferents capes de protecció** en diferents àmbits així com de **prevenció i resiliència** D'aquesta manera, es combinen diferents mesures per a prevenir i mitigar atacs de forma efectiva

1. Definició de ciberseguretat i importància per a les empreses i comerços

1.1 Definició de ciberseguretat

QUINA IMPORTÀNCIA TÉ?

Avui en dia, **les empreses i el comerços tenen una gran presència digital**, ja sigui exposada públicament a través d'Internet o internament mitjançant sistemes informàtics per gestionar les dades i processos interns.

No ser capaç de protegir-se efectivament contra les noves amenaces exposa les empreses actuals a la pèrdua d'informació confidencial, a un impacte negatiu, a **la incapacitat de desenvolupar l'activitat empresarial i a la vulneració de lleis específiques**, com el nou reglament de protecció de dades (**RGPD**), l'incompliment del qual **comporta sancions severes**

1. Definició de ciberseguretat i importància per a les empreses i comerços

1.2 Impacte dels ciberatacs

EL CIBERCRIM ESTÀ EN EXPANSIÓ:

Es calcula que l'any 2021 cada 11 segons hi hagut un ciberatac a nivell mundial. Aquesta dada ha augmentat significativament els últims anys: el 2016 la mitjana era de 40 segons.

El 99 % de les empreses espanyoles admet haver patit un ciberatac durant el 2020, amb una mitjana de cinc ciberatacs rebuts per empresa. El 43 % d'aquests atacs van dirigits a pimes.

El sector públic, el de l'energia i la indústria manufacturera han estat els sectors que més ciberatacs han rebut en el darrer any. Un altre sector que ha patit l'atac de hackers arran de la pandèmia ha estat el de proveïdors de salut.

- Font: Cybersecurity Outlook Report, VMWare Carbon Black
- Generalitat de Catalunya

1. Definició de ciberseguretat i importància per a les empreses i comerços

1.2 Impacte dels ciberatacs

PRINCIPALS IMPACTES NEGATIUS D'UN CIBERATAC PER A LES EMPRESES:

- El 45 % dels atacs a Espanya provoquen danys per valor de més de 400.000 €.
- El cost mitjà d'un atac a una pime és de 35.000 €.
- L'any passat, el 45 % de les empreses va haver de gestionar una interrupció de més de 5 hores a causa d'un ciberatac.
- El 18 % dels atacs a la seguretat han provocat que més de la meitat dels sistemes de l'empresa es vegin afectats.

- Font: Cybersecurity Outlook Report, VMWare Carbon Black
- Generalitat de Catalunya

1. Definició de ciberseguretat i importància per a les empreses i comerços

1.3 Qui hi ha al darrere el cibercrim?

PRINCIPALS MOTIUS DARRERE DELS CIBERATACS:

- Font: Raconteur.net 2021
- Font: Generalitat de Catalunya

1. Definició de ciberseguretat i importància per a les empreses i comerços

1.3 Qui hi ha al darrere el cibercrim?

EXEMPLES MÉS HABITUALS DE VIES DE MONETITZACIÓ QUE UTILITZEN ELS CIBERCRIMINALS:

- Clonació de targetes de crèdit
- Transferències bancàries
- Frau en assegurances o serveis mèdics
- Suplantació d'identitat a la xarxa amb finalitat comercial
- Robatori de criptomonedes
- Venda d'informació a terceres parts:
    - Propietat intel·lectual
    - Informació confidencial

- Font: Raconteur.net 2021
- Font: Generalitat de Catalunya

2. A què s'enfronten les empreses i els comerços actualment?

Podem classificar aquests mals en dues grans categories

- Els que **sostreuen informació de manera silenciosa** i, per tant, busquen romandre no detectats en els sistemes, per a **robar des de dades personals** (que després els cibercriminals poden revendre en els baixos fons d'Internet), fins a **números de compte, claus d'accés, i dades de targetes de crèdit de clients.**

- Programes de **malware que realitzen un mal actiu i visible de seguida**, com l'encriptació del contingut del disc dur dels ordinadors **i l'exigència d'un rescat** a canvi de desencriptar les dades.

En el pitjor dels casos, es combinen tots dos efectes: el robatori de dades, amb el segrest d'aquestes per a la subsegüent extorsió a l'empresa afectada.

3. Com entren aquestes amenaces en els nostres Sistemes informàtics?

Ho poden fer de dues maneres:

- **Explotant falles** en el nostre programari, des del sistema operatiu fins a les aplicacions (com qui troba una finestra que no ajusta i l'acaba d'obrir per a accedir a l'edifici).

- la **"enginyeria social",** i que no és res més que l'engany o l'estafa de tota la vida a les persones, per a aconseguir d'alguna manera accés als sistemes informàtics que aquestes gestionen.
  - Un exemple d'enginyeria social és el **phishing**
    - Una pràctica consistent a simular missatges de correu electrònic procedents d'una entitat bancària que conviden a fer clic sobre un enllaç per a finalitzar una operació bancària, comprovar unes dades, o reactivar un compte suspès temporalment.
    - Aquesta pràctica s'ha estès als telèfons intel·ligents amb el **smishing**, el mateix però amb missatges SMS.

3. Com entren aquestes amenaces en els nostres Sistemes informàtics?

En els últims anys, la proliferació d'ordinadors portàtils, telèfons intel·ligents i tauletes entre altres dispositius, que són d'ús personal però acaben també exercint funcions en l'empresa, s'ha disparat.

Fins a tal punt que **Costa dissociar el que és un ús purament personal d'un professional en un mateix dispositiu.** I, en la majoria de microempreses i Pimes, aquest ús és mixt, sense parlar ja dels treballadors autònoms.

4. 10 consells per a mantenir-nos ciberprotegits a l'empresa o la nostra botiga

1- Sensibilitzar i formar el personal de l'empresa en matèria de ciberseguretat.

La baula més feble en la cadena de la ciberseguretat acostuma a ser l'usuari, la persona, per això funciona l'abans esmentada **enginyeria social**. En aquest context, és imprescindible que els treballadors de l'empresa estiguin sensibilitzats sobre la seva part en la cadena de la ciberseguretat i disposin de formació sobre aquest tema en bones pràctiques, amb coses tan simples com no connectar pendrives USB externs en els sistemes corporatius.

2- Cal ser desconfiat.

Quan rebem un missatge de correu electrònic de la nostra entitat bancària o que ens convida a obrir un arxiu adjunt, hem de pensar-nos-el dues vegades: per què m'envien això? Correspon a una gestió que he iniciat jo o sé que estava en marxa? Si no és el cas, podem ignorar el missatge, o bé trucar per telèfon a qui ens l'envia per a comprovar que és legítim.

4. 10 consells per a mantenir-nos ciberprotegits a l'empresa o la nostra botiga

3- Hem de segmentar la xarxa

Igual que els grans vaixells estan dividits en compartiments perquè un forat en el casc no provoqui que tota la nau s'ompli d'aigua, una xarxa segmentada pot contenir una intrusió i que afecti el mínim d'equips.

4- Hem de comptar amb una administració professional de la xarxa.

Les tasques d'aquest administrador passaran, per exemple, per la gestió de l'accés als recursos, ja que si algú aconsegueix guanyar accés a un usuari, no pugui créixer per tot el sistema i l'agressió quedi, novament, continguda.

4. 10 consells per a mantenir-nos ciberprotegits a l'empresa o la nostra botiga

5- Hem de donar especial atenció als "nòmades digital".

Inevitablement, part del personal de l'empresa desenvoluparà el seu treball fora de l'oficina i, per tant, connectarà els seus ordinadors, telèfons intel·ligents i tauletes, tant a les xarxes corporatives com a les de fora. A més, quan estiguin fora, poden estar més desprotegits davant robatoris de dades o altres ciberatacs.

Cal **implementar mecanismes extra de protecció** a aquests perfils, com ara **VPNs** (Virtual Private Network, o xarxa virtual privada).

6- BYOD (Bring Your Own Device, o porta el teu propi dispositiu) quan el dispositiu personal també s'utilitza per a treballar.

En petites empreses i, especialment, en el cas dels treballadors autònoms, la frontera entre l'ús dels dispositius per a la vida personal i la vida laboral és molt flexible o, directament, inexistent. Això hem de tenir-ho molt en compte a l'hora de planificar la ciberseguretat.

4. 10 consells per a mantenir-nos ciberprotegits a l'empresa o la nostra botiga

7- Dimensionar i assegurar la nostra presència en internet i els serveis en línia que oferim.

Si la presència en línia de la nostra empresa és essencial per a la continuïtat del nostre negoci, i si **oferim algun tipus de servei en línia als nostres clients**, **un atac de denegació de servei (Dos, DDoS) podria deixar-los inutilitzats** per diverses hores i, fins i tot, dies. Això, a més **d'afectar la nostra facturació, també podria fer-ho a la nostra imatge**.

Necessitem **disposar d'un pla de mitigació d'atacs i continuïtat de funcionament**. Novament, els professionals del hosting i de la seguretat informàtica seran els nostres aliats.

8- Hem de monitorar els sistemes i la xarxa en temps real.

No fa falta que ens quedem tot el dia mirant un monitor a veure què passa: els sistemes moderns de protecció i antimalware disposen d'eines d'intel·ligència artificial que faran el treball per nosaltres i ens informaran de les amenaces bloquejades.

- Monitorar Firewall (Xarxa)
- Monitorar atcas equips (Bitdefender Gravity Zone)
- Monitorar Servidors cloud o *on premise*
- Monitorar pàgines web (WordPress, Prestashop...)

4. 10 consells per a mantenir-nos ciberprotegits a l'empresa o la nostra botiga

9- Hem d'actualitzar els nostres sistemes

Els cibercriminals també exploten **forats de seguretat en el nostre programari.**

Actualitzar les aplicacions que tenim instal·lades i el sistema operatiu porta al fet que els nostres ordinadors i dispositius vagin tancant aquests forats, impedint el pas als 'dolents'.

10- Necessitem un pla de continuïtat de l'empresa

Una **còpia de seguretat o backup està bé**, però realitzant únicament la còpia no anem a enlloc.

Cal fer-lo de forma planificada perquè, en qualsevol eventualitat, les dades de la còpia no resultin afectats, i **comprovar si els podem recuperar per a continuar treballant**

També hem de **disposar d'un pla d'acció** per a seguir amb la nostra activitat si no podem utilitzar els nostres ordinadors **en cas de sofrir un ciberatac.**

4. Consells per a mantenir-nos ciberprotegits a l'empresa o la nostra botiga

Font: Agéncia de ciberseguretat de Catalunya

4. 10 consells per a mantenir-nos ciberprotegits a l'empresa o la nostra botiga

Font: Agéncia de ciberseguretat de Catalunya

5. Política de seguretat informàtica

Què és una política de seguretat?

Un document en el qual s'hi plasmen les normes d'ús de tota la infraestructura tecnològica (que inclou el maquinari, el programari, la connectivitat,... tot, en definitiva) per tal que aquesta sigui segura.

L'objectiu és evitar atacs informàtics i intrusions, i reduir al màxim possible l'impacte d'aquells que resultin reeixits, garantint la integritat de les dades, la seva confidencialitat, i la continuïtat del negoci

5. Política de seguretat informàtica

Què és una política de seguretat?

Contempla tant les mesures de defensa passiva com les més proactives, així com defineix **què poden fer (i com fer-ho) els treballadors amb les infraestructures tecnològiques de l'empresa**, i què no han de fer mai. També té en compte **plans de contingència** per als pitjors casos, aquells en què un atac resulti totalment reeixit

És, en definitiva, **d'obligat coneixement i compliment per a tots els directius i treballadors de l'empresa**.

5. Política de seguretat informàtica

En què consisteix la política de seguretat?

Abasta tot el que fem i podem fer amb els sistemes d'informació corporatius, començant per marcar quins permisos d'accés tindrà el nostre usuari a cada recurs i com ens haurem d'identificar davant del sistema.

Inclou quin nivell de privilegis té cada usuari, a quins recursos pot accedir (emmagatzematge, dades, aplicacions, màquines,…), quines tasques i processos podrà dur a terme, i en quins grups d'usuaris (un concepte semblant a grups de treball) s'integra.

5. Política de seguretat informàtica

En què consisteix la política de seguretat?

El fet de **limitar accessos** no és un caprici: **si un atacant aconsegueix introduir-se** en un perfil d'usuari de la nostra xarxa, el mal que podrà fer estarà limitat pels permisos dels quals gaudeixi l'usuari "envaït", i per això **el mal que podrà fer l'atacant és limitat.**

Ara imagineu-vos que el nostre **usuari té permisos il·limitats** dins la xarxa: un atacant **podria accedir impunement** a totes les dades, robar-les, modificar-les, eliminar-les… un desastre, vaja!

5. Política de seguretat informàtica

En què consisteix la política de seguretat?

S'hi defineix com seran les claus d'accés i cada quant es canviaran; sí, allò tan pesat de "*ara l'ordinador em torna a demanar que canviï la contrasenya? Però si només fa un mes! la mare que el va…*"

Explica també **com ha de ser la seguretat perimetral**, quins han de ser els **sistemes antimalware** que emprarà la xarxa i els equips que la componen, **com es connectaran els usuaris des de fora** (per a teletreballar), emprant una **VPN**, i com i quan es duran a terme les **actualitzacions dels sistemes** i els programes.

5. Política de seguretat informàtica

En què consisteix la política de seguretat?

Pràctiques que no s'han de dur a terme de cap manera, per òbvies que semblin: **no compartir la contrasenya** amb ningú, **no descarregar ni instal·lar programes de pàgines web dubtoses** (cosa que el mateix sistema ja no hauria de deixar fer als usuaris si està ben configurat), o **vigilar amb el que se'ns demana que fem mitjançant un missatge de correu electrònic** (evitar pràctiques de phishing o de ransomware).

5. Política de seguretat informàtica

Per què cal tenir-la?

Qualsevol **empresa**, inclosa la vostra, treballa avui en dia amb un conjunt de **dades**, on s'hi inclouen les **de terceres parts**, que estan **sotmeses a una especial protecció**. Si, per inacció nostra, **es filtren les dades de clients**, proveïdors, o qualsevol altra que sigui de terceres parts, **la nostra empresa pot rebre una sanció**, i no pas precisament petita, amb totes les conseqüències que se'n desprenen tant per a la gerència com per als treballadors.

Si us gasteu uns diners en una alarma, si compreu les millors eines per poder crear un producte o servei de qualitat, **per què no invertir en un bon sistema informàtic degudament protegit?** El futur de la vostra empresa hi és dipositat.

6. Conclusió

Molta gent pensa que la seva empresa és massa petita per a convertir-se en objectiu dels cibercriminals. Però aquests no solament se centren en grans multinacionals, **i és més fàcil guanyar moltes petites quantitats de diversos robatoris selectius a petites empreses o professionals autònoms, que donar un gran cop.**

Així que sí, tots som objectiu potencial dels cibercriminals, hem de tenir-ho en compte per a protegir-nos i fer-ho bé.

Ayub Nakmoussi Harrak – Project Manager IT

972 462 999
anakmoussi@bdrinformatica.com

Finançat per la Unió Europea
NextGenerationEU