UNITAT DE CONEIXEMENT

Octubre 2020

Ciberseguretat i Recursos Humans

"Si creus que la tecnologia pot solucionar els teus problemes de seguretat, llavors no entens els problemes i no entens de tecnologia."

Bruce Schneier

fundació factor humà

Què és?

Tota organització té l'obligació de protegir la informació confidencial a la que té accés gràcies a l'exercici diari de la seva activitat. És per això que, especialment en un moment en què el teletreball s'ha convertit en quelcom massiu i les accions ofensives contra sistemes d'informació s'han incrementat significativament, les empreses han de posar el focus en la ciberseguretat i destinar-hi recursos.

- ✓ La **ciberseguretat**, també coneguda com a **seguretat de la informació electrònica** o **seguretat de tecnologia de la informació**, "és la pràctica de defensar els ordinadors, els servidors, els dispositius mòbils, els sistemes electrònics, les xarxes i les dades d'atacs maliciosos", tal com ho defineix la companyia internacional dedicada a la seguretat informàtica Kaspersky. Aquest concepte és aplicable tan en l'àmbit domèstic com al dels negocis i, en aquest darrer cas, implica especialment a dos departaments: el de Tecnologia de la Informació i el de Recursos Humans.

  - Tot i que tradicionalment s'ha relacionat aquesta matèria amb l'Àrea de Tecnologia de la Informació, la **funció de Persones** d'una organització també ha de tenir incidència en l'àmbit de la ciberseguretat, tenint en compte que una incorrecta manera de procedir per part dels membres de la plantilla pot generar una situació de vulnerabilitat per al sistema d'informació. Al mateix temps, és important tenir present que una de les millors mesures de prevenció de ciberamenaces que pot tenir qualsevol empresa és la formació i conscienciació de les pròpies persones treballadores. A més, el paper que juga també pot ser clau en cas que no s'hagi pogut evitar que l'empresa sigui víctima d'un ciberatac, essent fonamental en la seva gestió.

  - **Què pot fer el Departament de Recursos Humans per implicar-se en la prevenció i gestió de ciberatacs?** Tal i com s'explica en el blog "Más que nómina" de la companyia Seresco, l'Àrea de Persones pot **organitzar jornades de conscienciació** entre els/les empleats/des per tal que entenguin millor quins són els riscos i, a més, pot **facilitar una formació en seguretat** adequada al seu nivell. D'altra banda, és important que participi en la **revisió dels procediments de seguretat** amb l'objectiu de millorar la seva adaptació als diferents llocs de treball i que **revisi els procediments d'alta i baixa de les persones treballadores** per assegurar que s'estiguin fent correctament. Finalment, aquest Departament també pot tenir un paper essencial a l'hora de **realitzar simulacres d'atacs**

per enginyeria social, que permeten avaluar el grau de conscienciació dels/de les treballadors/es respecte aquest tipus d'amenaces.

- Pràctiques com aquesta última són cada cop més habituals en les empreses. És per això que la figura del ***hacker* ètic** ha agafat rellevància en els darrers temps. Tal i com s'exposa en el blog d'Iberdrola, els *hackers* ètics tenen com a objectiu reforçar la seguretat informàtica de les organitzacions duent a terme atacs que permetin avaluar-la. Generalment són part de la plantilla de grans empreses però també pot tractar-se de professionals externs que actuen com a consultors a través d'empreses de ciberseguretat. Gràcies al *hacking* ètic les organitzacions poden detectar vulnerabilitats i estan molt més preparades en cas que la ciberamenaça sigui real.

- En definitiva, és evident que la ciberseguretat és una qüestió transcendent per a les organitzacions. Tot i això, l'increment de mesures aplicades per les empreses pot fer aflorar un nou debat: és possible que s'utilitzi l'argument de la seguretat per tal de sotmetre les persones treballadores a un major control? És fonamental que les organitzacions trobin l'equilibri entre la privacitat de les persones i la seguretat de l'empresa.

Eines

Per tal d'evitar que el sistema d'informació d'una empresa pateixi ciberatacs, o com a mínim reduir-ne el risc, és important que tant els/les empleats/des com la pròpia organització adoptin les mesures de protecció i prevenció adients. Segons s'exposa en l'article de la revista Capital Humano basat en una guia elaborada per EY *Diez medidas para protegerse de los ciberataques en tiempos de la Covid-19*, algunes de les mesures més recomanables son:

- **Utilitzar sempre que sigui possible els ordinadors de l'empresa**, ja que disposen de les mesures de seguretat òptimes. En cas que no sigui possible i s'hagi d'optar per utilitzar ordinadors personals, es recomana que el Departament de Tecnologia de la Informació els doni prèviament el vistiplau.

- **Gestionar i utilitzar adequadament el correu electrònic,** extremant les precaucions en l'enviament d'*e-mails* externs a l'organització i evitant fer ús de mitjans la seguretat dels quals ens generi dubtes.

- **Mantenir al dia les actualitzacions de seguretat** relatives a sistemes operatius, versions del navegador d'Internet i les extensions i

complements. Si la persona treballadora evita tenir un software obsolet, les probabilitats de patir atacs es redueixen.

- ✓ **Fomentar un accés acurat a la informació que està a disposició de l'organització per dur a terme l'activitat diària.** EY considera que aquesta mesura és especialment rellevant en l'actualitat degut a l'auge del teletreball i on tant les empreses com els/les empleats/des tenen part de responsabilitat:
  - Les **organitzacions** han de compatibilitzar l'ús d'eines col·laboratives amb la protecció i la seguretat de la informació.
  - Els/les **treballadors/es** han d'evitar descarregar o emmagatzemar informació corporativa en equips personals.
- ✓ **Establir regles sòlides de seguretat i monitoritzar els accessos i connexions** per tal de detectar qualsevol activitat considerada estranya o perjudicial en matèria de seguretat.
- ✓ **Gestionar adequadament les contrasenyes,** fent que aquestes siguin llargues i complexes. També es recomana que només siguin conegudes pel/per la treballador/a, que es canviïn de manera freqüent i que no es reutilitzin aquelles que ja s'han emprat anteriorment.
- ✓ **Comptar amb programes antivirus en tots els equips i mantenir-los actualitzats.**
- ✓ **Garantir la seguretat en la connexió remota,** fent ús sempre que sigui possible d'una Xarxa Privada Virtual (XPV). Si les connexions es realitzen des de casa, cal assegurar-se que l'accés a la WI-FI sigui a través d'una contrasenya robusta. A més, és important protegir amb contrasenya els enviaments d'arxius que contenen informació sensible per a l'organització.
- ✓ **Evitar obrir correus i enllaços d'origen desconegut, desconfiar de peticions de dades personals o credencials d'accés i descarregar únicament aplicacions per al telèfon mòbil a través de pàgines web oficials.** D'aquesta manera, es poden evitar dos tipus d'atacs dirigits molt habituals:
  - **La infecció amb *malware*,** que pot conduir al control de l'ordinador de manera remota i al robatori d'informació a través d'un software espia.
  - **El *phishing* o *spear phishing*,** que permet l'obtenció sense autorització de credencials d'accés a banca *online*, targetes de crèdit, etc.
- ✓ **Assegurar-se de la veracitat de la informació rebuda i evitar difondre informació falsa.**

La dada

La implantació massiva del teletreball a causa de la pandèmia de la Covid-19 ha obert noves bretxes de seguretat a les empreses, com evidencien les dades que proporciona l'equip de seguretat d'IBM referents al primer trimestre de 2020:

- ✓ A **nivell mundial**, la **quantitat d'atacs informàtics va augmentar en un 40%** en comparació amb el mateix període de l'any anterior.
- ✓ En el cas d'**Europa**, l'augment del nombre de ciberatacs és encara més impactant, assolint un **creixement del 125%** respecte l'any anterior.

Però **no només el teletreball augmenta el risc de patir ciberatacs.** Tant si es treballa en remot com presencialment, **és essencial el paper dels/de les treballadors/es.** Queda palès a través d'una investigació realitzada per l'Stanford University i la firma de ciberseguretat Tessian, que alerta que:

- ✓ La **fatiga** i l'**estrès** dels/de les professionals repercuteixen directament en la ciberseguretat. Aquesta qüestió és especialment rellevant tenint en compte que **el 93% de les persones enquestades reconeix sentir cansament i estrès durant la seva jornada laboral.**

Guia de Treball

PRIMERS PASSOS PER REDUIR EL RISC DE PATIR CIBERATACS

Segons s'explica en l'article *Medidas clave para garantizar la ciberseguridad en la empresa*, publicat en la web de la firma de serveis professionals BDO, per tal d'evitar possibles atacs virtuals i mitigar-ne els danys en cas que aquests s'acabin produint, és fonamental que les organitzacions posin el focus en la ciberseguretat:

- **Implementant accions focalitzades en el xifratge de la informació** i **realitzant regularment còpies de seguretat.**
- **Desenvolupant protocols d'actuació que permetin respondre amb agilitat en cas de ciberatac.** Per afavorir aquesta resposta ràpida, és fonamental organitzar i jerarquitzar prèviament les dades per facilitar-ne el rastreig.
- **Vetllant pel correcte compliment de tots els protocols i mesures:** és important que les empreses duguin a terme avaluacions periòdiques en totes les seves àrees i departaments. D'aquesta manera, es podrà garantir una seguretat real.

ELS/LES PROFESSIONALS: LA CLAU PER ACONSEGUIR UN ENTORN VIRTUAL SEGUR

El paper de les persones és bàsic a l'hora de garantir la seguretat en l'entorn virtual. En conseqüència, és necessària la implicació directa la funció de Persones a través d'accions com:

- **La identificació, atracció i retenció de talent professional:** cal que les organitzacions comptin amb professionals qualificats, tant enginyers experts en TI com altres perfils, per exemple, politòlegs o criminòlegs. D'aquesta manera, es podrà entendre el que hi ha darrere de cada ciberatac (motivació, model econòmic, perfil de l'atacant, etc.) i serà possible millorar la capacitat de resposta.
- **La integració del talent qualificat a les estructures corporatives:** és fonamental que els/les professionals encarregats/des d'evitar qualsevol atac als sistemes d'informació se sentin recolzats dins de l'organització i puguin treballar amb totes les facilitats possibles. Tot i això, en moltes organitzacions, tal com s'exposa en l'article de l'Observatorio de Recursos Humanos *El déficit de talento en ciberseguridad incrementa los riesgos digitales de las empresas*, topen amb certa falta de sensibilització corporativa i, a més, treballen amb un pressupost limitat i han de dedicar molt temps a realitzar tasques de compliment normatiu.
- **La conscienciació i formació del conjunt de les persones empleades en matèria de ciberseguretat.**

L'experiència

ElTenedor és una plataforma fundada l'any 2007 a través de la qual es poden efectuar reserves en restaurants de forma gratuïta i en temps real. La companyia, que des de l'any 2014 forma part de TripAdvisor Media Group, compta amb unes 900 persones empleades i opera en 17 països d'arreu del món. Un dels principals èxits d'ElTenedor rau en la participació dels/de les usuaris/es i la dels/de les restauradors/es, ja que l'aplicació recull valoracions i informacions proporcionades per tots/es ells/es amb la finalitat de facilitar la cerca del restaurant idoni per a cada moment.

- ✓ La plataforma va llançar una promoció coneguda com "**The yummy days**", que consistia en un joc diari que permetia guanyar durant una setmana un àpat gratis valorat en un màxim de 120 euros i diversos premis en forma de *Yums*. Cal destacar que els *Yums* son punts que s'obtenen en reservar a través d'ElTenedor i que es poden bescanviar per descomptes en els restaurants que hi estan associats.

- ✓ Tal i com s'explica en l'article de Medium *An Ethical Hacking Story – The Yummy Days Case*, l'enginyer i desenvolupador d'aplicacions web Héctor Martos va detectar gairebé per casualitat un **problema de seguretat a nivell tecnològic** en aquesta promoció.

  - Per participar-hi, era necessari omplir un formulari on es demanava el correu electrònic i calia acceptar les condicions d'ús. Un cop realitzat aquest pas i havent participat en el joc que proposava la plataforma, es podia saber si s'havia guanyat algun premi o no. En una de les ocasions que l'enginyer va omplir el formulari, va percebre que podia veure fàcilment la URL a la que estava accedint.

  - Gràcies als seus coneixements, va observar que la interfície de l'usuari estava fent sol·licituds a un servidor API. Va decidir, doncs, guardar les sol·licituds i respostes i va provar de jugar novament introduint el seu correu electrònic. No va ser possible, ja que se'l redirigia a una pàgina que especificava que ja havia participat anteriorment. Tot i això, si que va poder participar-hi amb una altra adreça de correu no registrada a l'aplicació d'ElTenedor. Segons explica el propi enginyer, "l'API no validava si el correu introduït estava registrat a l'aplicació o no". Així doncs, podia jugar una i altra vegada amb direccions diferents per intentar guanyar més premis.

  - Aquesta no és una problemàtica especialment greu si pensem en una persona que participa repetidament en la promoció introduint manualment diferents *mails*. Segons el desenvolupador d'aplicacions web, el veritable problema de seguretat per a la plataforma té a veure amb la possibilitat d'automatitzar aquest procés i repetir-lo cada segon. Héctor Martos va decidir posar-ho en pràctica i demostrar que podia guanyar diversos premis de forma automàtica. Ho va aconseguir i, posteriorment, en va informar a la plataforma per tal que poguessin solucionar la vulnerabilitat detectada.

- ✓ Cal tenir en compte que si l'enginyer no hagués notificat el problema i més participants haguessin detectat aquesta vulnerabilitat, s'hauria posat en entredit la **seguretat** de la plataforma, la qual cosa hauria pogut afectar negativament la **reputació del negoci**.

Charter of Trust és una iniciativa impulsada per la multinacional alemanya Siemens que ha aconseguit unir els esforços de 16 empreses més, que operen a nivell internacional i en múltiples sectors, amb el propòsit d'assolir un entorn digital més segur. Aquesta iniciativa va sorgir en el marc de la Conferencia de Seguretat de Munich de l'any 2018 per tal de "protegir les dades de particulars i empreses, prevenir danys a persones, organitzacions i infraestructures i crear uns fonaments fiables sobre els quals la confiança en la Xarxa pugui créixer", tal com exposen des de la seva pròpia pàgina web. Entre les signants de la carta hi destaquen empreses com Airbus, Allianz, IBM, Atos i Mitsubishi Heavy Industries, entre d'altres.

- ✓ En els últims mesos el teletreball s'ha convertit en una opció laboral utilitzada de forma massiva degut a la pandèmia de coronavirus i ha estat necessari posar el focus en la **ciberseguretat**, ja que la fiabilitat i seguretat dels entorns virtuals treballant des de casa no és la mateixa que des de les oficines i els *hackers* poden aprofitar aquest tipus de vulnerabilitats. Per això, la iniciativa Charter of Trust ha donat a conèixer **8 consells** que han de permetre **mantenir l'activitat habitual dels negocis mentre es treballa *online*** i, alhora, **prevenir possibles ciberatacs.**

  - **Recomanacions dels socis de Charter of Trust,** que es poden consultar a través de la seva pàgina web:

    - ❖ Endur-se a casa només aquells dispositius que són imprescindibles i consultar i utilitzar només la informació necessària.
    - ❖ Mantenir el software actualitzat en tots els dispositius.
    - ❖ Optar només per comunicar-se de forma segura i protegint la xarxa domèstica.
    - ❖ Utilitzar els dispositius d'ús empresarial només per a la realització de l'activitat laboral i reservar la utilització dels dispositius personals per a l'ús no professional.
    - ❖ Apagar els dispositius intel·ligents controlats per veu que es troben en l'entorn de treball i cobrir la càmera web quan no està en ús.
    - ❖ Identificar proactivament les persones participants en les reunions realitzades per videotrucada.

- Tancar la sessió quan el dispositiu no està en ús i guardar-lo de forma segura.
- Tenir especial cura en obrir correus electrònics i arxius adjunts que es puguin considerar sospitosos, sobretot si no es coneix al remitent.

Materials

Bibliografia bàsica

Arreola, Adolfo. *Ciberseguridad: ¿Por qué es importante para todos?* Barcelona: Siglo Veintiuno editores, 2019

Dans, Enrique. *Viviendo en el futuro. Claves sobre cómo la tecnología está cambiando nuestro mundo.* Bilbao: Deusto, 2010

Stephens-Davidowitz, Seth. *Todo el mundo miente. Lo que Internet y el Big Data pueden decirnos de nosotros mismos.* Madrid: Capitán Swing, 2019

Materials en línia

Ciberseguridad en el teletrabajo: Una guía de aproximación para el empresario

Guia elaborada per l'Instituto Nacional de Ciberseguridad (Incibe) amb l'objectiu d'ajudar les organitzacions a garantir l'accés segur dels/de les treballadors/es als sistemes d'informació de l'empresa mentre treballen en remot. En aquest document s'hi exposen els principals riscos del teletreball en matèria de ciberseguretat i, a més, s'hi recullen algunes recomanacions i mesures per protegir la informació.

https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberseguridad_en_el_teletrabajo.pdf

Doménech, Enric. "Mesures clau per garantir la ciberseguretat a l'empresa". *BDO España*, 22/11/2019.

Article de la firma de serveis professionals BDO que recull un total de 9 mesures preventives que tenen com a objectiu reduir el risc de patir ciberatacs o, com a mínim, minimitzar els danys causats per l'apropiació indeguda d'informació i de dades.

https://www.bdo.es/es-es/publicaciones/articulos/medidas-para-garantizar-la-ciberseguridad

Kit de conscienciació per a empreses, de l'Instituto Nacional de Ciberseguridad (Incibe)

Recursos didàctics i eines d'entrenament que l'Instituto Nacional de Ciberseguridad (Incibe) posa a disposició de les organitzacions, especialment de les pymes i les microempreses, per facilitar la conscienciació i la formació de les seves plantilles en matèria de ciberseguretat. Aquest kit és aplicable a empreses de tots els sectors i sense necessitat de tenir coneixements tècnics previs.

https://www.incibe.es/protege-tu-empresa/kit-concienciacion

Unitats de Coneixement relacionades

- Teletreball (2020): https://factorhuma.org/unidades-de-conocimiento-blog/14574-teletreball
- Adaptació a la nova Llei de Protecció de Dades (2018): https://factorhuma.org/unidades-de-conocimiento-blog/13746-adaptacio-a-la-nova-llei-de-proteccio-de-dades