TECNOLOGIA

SEGURETAT INFORMÀTICA: Creus que la teva empresa està segura?

hst t'ajuda

A l'empresa HST fa més de 18 anys que ens dediquem a assessorar a empreses en l'àmbit de la informàtica, de la seguretat i de la protecció de dades. Treballem en tot moment perquè el client d'HST tingui a les seves mans tot un ventall de recursos per millorar el seu rendiment mitjançant la tecnologia i el dotem de les eines necessàries per optimitzar els seus resultats, així com garantir la seguretat informàtica dels seus sistemes.

Cada setmana llegim a la premsa, articles sobre **atacs de ciberseguretat** a tot tipus d'empreses i sectors i, no queda lluny el record dels **virus massius,** com per exemple el Wannacry.

Segons dades de Panda Security, **un 43% dels atacs registrats a nivell global són a petites i mitjanes empreses.** El motiu es regeix a que aquestes acostumen a estar menys preparades i per això són percebudes com un blanc fàcil. Cal destacar però, què un atac cibernètic **no només posa en perill les dades dels clients o la privacitat** sinó que també, té c**onseqüències per l'empresa que el pateix.**

Costos i possibles penalitzacions

El passat mes de maig va entrar en vigor el nou reglament general de protecció de dades. Aquest contempla multes de fins a **un 4% del volum de negoci anual** per les empreses que no compleixin amb la llei de protecció de dades. Per aquest motiu, cal tenir en compte les possibles penalitzacions i treballar per prevenir un possible atac informàtic. **Les dades s'han d'emmagatzemar de manera segura i adequada.**

Problemes comercials i de temps

El robatori de dades o d'informació d'empreses acaba provocant **una pèrdua de temps per a la restauració i/o solució del problema**. Segons l'ICAEW, les petites i mitjanes empreses interrompen entre 7 i 10 dies les seves operacions com a conseqüència d'un ciberatac. Les repercussions són **importants a nivell comercial i a nivell estratègic** ja que, si no es preveu, pot afectar a tots els nivells de l'empresa.

Reputació

El 89% de les empreses que han tingut un atac cibernètic admeten que la seva reputació s'ha vist afectada. Un 30% reconeix que ha patit pèrdua de clients i un 29% haver de suportar la falta de capacitat per generar negoci. Unes dades que mostren com **la reputació d'una empresa es pot veure afectada en el cas d'un ciberatac,** així com també el desenvolupament d'una percepció negativa i la sensació de rebuig. **Les amenaces no només tenen efectes a l'empresa** sinó que, **pot involucrar als clients en cas de robatori de dades.**

Per tant, es recomana a totes les empreses i sobretot a les pimes, realitzar tasques de prevenció en ciberseguretat i emmagatzemar les dades sensibles de forma acurada i segura.

DECÀLEG PER TENIR LA TEVA EMPRESA CIBERSEGURA

1.- **Definir un pla de seguretat i contingència:** Analitzar l'estat de seguretat i definir on volem arribar. Això es plasmarà en una sèrie de polítiques i normatives que dirigiran la forma d'abordar la seguretat en el seu dia a dia.

2.- **Usuaris i passwords segurs per accedir als sistemes:** Ficar en marxa i/o millorar el sistema de control d'accessos lògics, ja que igual que controlem qui entra a les nostres instal·lacions, hem de controlar qui entra en els nostres sistemes.

3.- **Còpies de seguretat:** Les còpies de seguretat han de prevaldre a tot tipus d'empreses i han de ser com a mínim diàries, encriptades i emmagatzemades fora de les instal·lacions. És la forma de recuperar-se de gairebé qualsevol incident. Actualment, la millor opció són les còpies al núvol.

4.- **Antivirus i protecció antimalware:** Els virus muten per fer-se cada vegada més nocius i perillosos i ens hem de protegir. Cap pime està exempta d'aquest risc, ja que no hi haurà protecció eficaç si fem servir sistemes o aplicacions obsoletes i desactualitzades, aquest tipus d'aplicacions són més vulnerables que la resta.

5.- **Sistemes operatius i aplicacions actualitzades:** Com hem dit en el punt anterior, cal utilitzar sistemes i aplicacions de versions més actuals i amb suport i actualitzacions per part del fabricant.

6.- **Tallafocs:** La nostra xarxa ha d'estar protegida per evitar tot tipus d'intrusions en els sistemes. I com l'accés de de l'exterior de clients i col·laboradors es fa imprescindible en un mitjà comercial electrònic, no es pot descuidar la seguretat de la informació quan és comunicada cap i des de l'exterior. Això ho aconseguirem mitjançant la instal·lació d'un firewall o tallafocs.

7.- **Seguretat dels dispositius mòbils i servidors:** Cal protegir la informació emmagatzemada en tot moment, ja que els suports poden extraviar-se o deteriorar-se. Controlar els suports de la informació durant tota la seva vida útil és també una mesura de seguretat elemental.

8.- **Registres d'activitat:** Ficar mitjans per dur a terme un registre d'activitat, on es pugui observar com interaccionen els usuaris amb els sistemes i detectar anomalies en el seu comportament.

9.- **Compliment de normatives de protecció de dades:** l'entrada en vigor del RGPD obliga a complir una sèries de mesures i protocols de seguretat de les dades.

10.- **Conscienciació als usuaris i sentit comú:** Tant els usuaris d'oficina de la teva empresa com el personal de producció ha de ser conscient i adoptar el sentit comú per vetllar per la ciberseguretat. Cal informar-los dels possibles perills en seguretat informàtica.

CONSELLS DE SEGURETAT INFORMÀTICA PER PARTICULARS I MICROPIMES

- **Realitzar, de tant en tant, una anàlisi amb un antivirus** dels teus equips i, de forma anàloga, de tots els fitxers que et descarregues.
- **Mantenir actualitzats els sistemes operatius i el programari dels dispositius** que utilitzis, sempre que sigui possible. Descarrega el programari només des de les pàgines i mercats oficials.
- **Sigues proactiu i crític amb tot el que apareix a la xarxa,** no donant credibilitat a tot el que aparegui publicat a internet sense contrastar la veracitat de les notícies, ni difonent rumors o notícies falses.
- **Informa't sobre les últimes amenaces i fraus que circulen per internet.** T'ajudaran a estar més protegit.
- **No facis clic als enllaços que apareguin als correus electrònics no sol·licitats** o que el remitent sigui desconegut, així evitaràs ser víctima de fraus i malware.
- **No utilitzis la mateixa contrasenya** en tots els serveis en línia que facis servir, no és una pràctica segura.
- **Estableix un doble factor d'autenticació,** Per a una major seguretat en els teus processos d'accés, També pots recolzar-te en un gestor de contrasenyes per a protegir de forma segura i senzilla les claus que utilitzis en els diferents serveis d'Internet.
- **Comprova les opcions de privacitat dels teus perfils a les xarxes socials,** és a dir, allò que altres persones poden veure quan accedeixen al teu perfil. Recorda, el més important és que pensis abans de publicar alguna cosa, ja que una vegada que comparteixis la informació serà difícil que puguis mantenir el control sobre ella.
- **Realitzar còpies de seguretat de la informació que emmagatzemes als teus dispositius**. D'aquesta manera, en cas d'intrusió (hackeig), pèrdua o robatori del dispositiu sempre podràs recuperar les teves dades ■

Des d'HST et convidem a revisar el teu sistema de seguretat informàtica perquè no hagis de patir per les teves dades. Els nostres experts vetllen contínuament per tenir les polítiques de seguretat informàtica el més actualitzades possibles per poder detectar atacs.

Realitzem auditories de seguretat i donem a les empreses els serveis necessaris per tal de mantenir els seus sistemes segurs en tot moment.

Si la teva empresa necessita una auditoria de seguretat i vols conèixer de la mà d'un expert l'estat de seguretat informàtica, a HST t'ajudarem.

No ho dubtis i demana més informació:

Truca al 973 72 71 72

o envia un mail a info@hst.cat

Jordi Rabinat · Director Tècnic d'HST