El Lloc de Treball

El lloc de treball és el lloc on es realitza la feina diària. Com parteix de les tasques quotidianes, qualsevol usuari requereix accés a certs sistemes i manipular diferents tipus d'informació. Com a conseqüència directa, hem de tenir en compte que el lloc de treball és un **punt clau** des del punt de vista de la **seguretat de la informació**.

Per això, és necessari que apliquem un conjunt de mesures de seguretat que ens garanteixin que la informació, tant de suport paper com en format electrònic, està correctament protegida.

1. Gestió de la documentació

Habitualment, quan pensem que un lloc de treball estàndard, ens ve a la ment un lloc de treball en una oficina, una taula de treball, caixoneres, etc.

Tot i això, molts de nosaltres treballem també, de manera parcial o total, en llocs de treball ubicats en entorns susceptibles de danyar la informació en suport paper.

Per evitar això, hem de prendre una sèrie de senzilles mesures preventives:

- Emmagatzemar o guardar la nostra informació en una ubicació adequada. Evitar un acostament a sistemes de refrigeració, canalitzacions d'aigua o instal·lacions que puguin afectar el paper.
- Utilitzar elements adequats per emmagatzemar paper, com per exemple, armaris, caixoneres que disposin de dispositius de tancament, o caixes fortes o armaris ignífugs en cas necessari.
- Destruir la documentació de manera segura. Depenen del volum de paper, podem utilitzar destructores de paper convencionals o subcontractar la retirada i destrucció a un proveïdor. En aquest últim cas no oblidar firmar el document de confidencialitat pertinent i sol·licitar els certificats de destrucció segura.

2. Contrasenyes segures

Hem de fer una política de contrasenyes segures, que defineixi almenys els següents aspectes de les claus que utilitzem:

- La longitud mínima de les claus.
- L'obligació d'utilitzar majúscules, minúscules i símbols.
- La periodicitat amb què s'ha de canviar les incidències.

Un exemple de contrasenya segura seria una clau d'accés amb una longitud mínima de 12 caràcters, composta per una combinació de lletres majúscules, minúscules, números i símbols.
També hem de recordar que les contrasenyes són personals, secretes i intransferibles. No hem d'apuntar-les en posts-its, llibretes, documents de text o qualsevol altre mitjà que permeti accedir fàcilment a les nostres claus. En el cas que necessitem que un company accedeixi a informació que gestionem, podem posar en funcionament mesures alternatives, com utilitzar repositoris compartits o informar els usuaris d'un segon contacte.

3. Mesures d'identificació

Una mesura d'autentificació és la tècnica o procediment que un sistema utilitza per a verificar que un usuari és qui diu ser.

Per portar a terme aquesta verificació, existeixen dos mètodes:

- Els basats en alguna cosa que sabem. El cas més evident és la utilització de contrasenyes.
- Els basats en alguna cosa que tinguem, com per exemple, una targeta d'accés magnètica.
- Els basats en alguna característica física de la persona, com per exemple, una empremta dactilar, retina o trets facials.

Com més mètodes combinem per l'accés a un sistema, més robust i fiable serà aquest. És a dir, més difícil serà falsejar-lo i trencar-lo.

Un exemple de mètode d'autentificació combinada seria establir un control d'accés al sistema en el qual l'usuari deu fer ús d'una targeta magnètica (alguna cosa que tenen) i addicionalment, s'hagi d'introduir un pin o contrasenya (alguna cosa que sap).

4. Política de taules netes

Diàriament treballem amb una gran quantitat de documentació, que és habitual que estigui distribuïda per sobre la taula, per a major comoditat o perquè és necessària per a feines diàries.

Tot i això, quan s'acaba la jornada hem de guardar la documentació que es trobi a la vista (informació de l'organització, usuaris, proveïdors, etc.). Això es especialment important si treballem en entorns compartits amb altres organitzacions, o fins i tot públics (atenció a l'usuari, per exemple). D'aquesta manera evitarem mirades indiscretes que puguin derivar en la fuita d'informació, a més del robatori de documents que puguin contenir informació confidencial.

Una política de taules netes requereix que:

- El lloc de treball ha de ser net i ordenat.

- La documentació que no estiguem utilitzant en un moment determinat ha de ser guardada correctament, especialment quan deixen el nostre lloc de treball i en finalitzar la jornada.
- No hi hagi usuaris ni contrasenyes apuntades en post-it o similars.

A més, encara que no sigui una mesura específica de taules netes, si abandonem el nostre lloc de treball, hem de bloquejar l'equip per evitar accés no autoritzat.

5. Enginyeria social

Els atacs d'enginyeria social tenen com a objectius a qualsevol treballador, sense importar el lloc en què treballi. A través d'ells, un atacant pot obtenir informació confidencial de les mateixes víctimes, o utilitzar-les per accedir a altres persones de l'organització de manera inadvertida.

Existeixen quatre pilars dels atacs d'enginyeria social, que permeten que en molts casos aquests tenen èxit:

a) El desig d'ajudar a altres persones.
b) La confiança que les persones actuen per bona voluntat.
c) El no voler dir que no a les peticions d'altres persones.
d) El desig de ser afalagat.

La millor manera d'entendre el que significa un atac d'enginyeria social és mitjançant un exemple, que veurem a continuació.

Suposem que un treballador del Departament de RRHH sense unes responsabilitats rellevants rep una trucada d'una persona que li indica que el truca del departament d'informàtica, tot i que en realitat es tracta d'un atacant. Després d'una breu conversa, l'atacant pot sol·licitar la informació sobre l'equip, la política d'actualitzacions, els programes instal·lats, o fins i tot sol·licitar l'usuari i contrasenya per a realitzar el manteniment de l'equip. A partir d'aquest moment, l'atacant podria portar a terme accions com intentar accedir als sistemes corporatius, instal·lar un troià o registrar totes les pulsacions del teclat.

Encara que sembli alguna cosa fruit de la casualitat, els atacs d'enginyeria social es porten a terme de forma planificada, obtenint informació de múltiples fonts, el que permet simular un coneixement similar al que tindria algú que treballés en l'organització.

Un dels medis més utilitzats en l'enginyeria social és el correu electrònic. Sota qualsevol pretext o excusa invita a l'usuari a enviar informació personal o de l'organització, fent clic en algun enllaç o a obrir un fitxer infectat adjunt.
L'atac per correu electrònic es realitza través d'un compte fals amb característiques similars als comptes de correu de l'organització, per donar-li més credibilitat en cas de ser un atac dirigit contra aquesta. Per exemple l'atac per correu electrònic en el qual s'indica que, a causa d'una auditoria que s'està portant a terme dins de l'organització en aquest moment. Qualsevol pretext es bo per invitar al treballador a executar l'arxiu que s'inclou en el correu electrònic.

Una altra de les tècniques utilitzades i que podem incloure dins d'aquest tipus d'atac a organitzacions, és l'ús de memòries USB "extraviades" com atac d'enginyeria social. Consisteix en deixar en llocs estratègics USBs amb fitxers infectats. Aquests estan identificats amb noms atractius, com per exemple, *NóminesFeb2014, auditoria_interna.exe* o similars, amb l'objectiu d'atraure la curiositat del treballador i que s'executin els fitxers.

Això fa que aquests atacs siguin molt difícils de preveure i, per tant, els de major probabilitat d'èxit. Hem d'estar alerta davant qualsevol activitat o sol·licitud sospitosa. Quina és la millor eina contra aquest tipus d'atacs? **El sentit comú**.

6. Fuites d'informació

La majoria de les fuites d'informació que es produeixen en les organitzacions tenen com a origen el lloc de treball del treballador. Poden ser fruit d'actes malintencionats per part dels treballadors descontents, o com d'errors a l'utilitzar els sistemes que gestionen la informació.

Per evitar les fuites d'informació, hem de ser cautelosos a l'hora d'utilitzar el correu electrònic i les xarxes socials.

Per exemple, les aplicacions per gestionar el correu electrònic acostumen a tenir la possibilitat d'autocompletar la direcció del destí. Si no som cautelosos, és possible que enviem accidentalment informació confidencial a un destí inapropiat.

Per una altra banda, en xarxes socials professionals és habitual que alguns usuaris incloguin informació sobre usuaris o projectes en els quals estan treballant, proporcionant valuosa informació que pot ser utilitzada per organitzar un atac d'enginyeria social entre altres.

Actualment existeixen solucions informàtiques amb l'objectiu principal de reduir el risc de les fuites d'informació, però hem de tenir en compte que cap eina és capaç de substituir al ja esmentat sentit comú a l'hora de gestionar la informació.