Restricted

APOLO ANALYTICS

LightEyes laSalle Technova Barcelona

Bons costums en l'entorn digital (objectiu 20/20)

1. Control d'accés al dispositiu.
   Haurem d'activar un control d'accés quan s'inicïi o arrenquem el nostre dispositiu, sigui mitjançant un PIN o un usuari i contrasenya en funció del dispositiu.
   De la mateixa manera que s'ha d'activar un control d'accés a l'inici del dispositiu, s'ha de definir una autenticació per al desbloqueig, sigui mitjançant PIN, patró o biomètric.

2. Activació de bloqueig automàtic.
   Perquè el dispositiu es bloquegi cal definir un temps d'inactivitat, després del qual es bloquejarà i no es podrà utilitzar sense el seu desbloqueig.

3. Encriptar el disc dur, SSD, Pendrive.
   El sistema operatiu ens proporciona mètodes d'encriptació (en Windows el Bitlocker), però existeixen softwares diversos que ens encripten el disc dur i fins i tot poden ocultar una part d'ell. Òbviament cal recordar molt bé la password o paraula clau, si no volem tenir un disgust.

4. Posar una contrasenya de BIOS.
   La BIOS és un software que permet l'arrencada de l'equip. Si bloquegem la BIOS amb una contrasenya, no es podrà iniciar el S.O. des d'aquest ordinador. Això és un complement de seguretat que a més permet que un lladre no pugui iniciar una unitat externa per a extreure dades o reinstal·lar el sistema. En definitiva, es quedaran amb un bonic i car petjapapers.

5. Ús de fonts de confiança per a la descàrrega d'aplicacions
   Les aplicacions que instal·lem en els nostres dispositius han de ser descarregades des de les botigues de Google o Apple. Descarregar aplicacions des de fonts de tercers és un risc que no hem d'assumir. Òbviament descarregar pel·lícules o documents de fonts il·lícites, a més de ser il·legal, és un perill màxim d'arrossegar tots els virus del món.

6. Permisos de les aplicacions.
   En instal·lar una aplicació, durant el procés d'instal·lació i amb les últimes versions del sistema operatiu, se'ns demanarà donar permís a aquestes, per exemple, d'accés a la càmera o a la nostra ubicació.

Restricted

7. Actualitzacions.

   Les actualitzacions d'aplicacions o sistemes operatius haurien de programar-se perquè es facin de manera automàtica. Les actualitzacions per norma inclouen millores de funcionalitat, però en alguns casos, incorporen millores de seguretat per a la nostra protecció.

8. Còpies de seguretat.

   Com ja hem esmentat, les còpies de seguretat sempre ens salvaran en cas de desastre. No hem d'obviar aquest punt i programar còpies periòdiques de seguretat que s'emmagatzemin en el núvol o en un altre dispositiu.
   Periòdicament, com a simulacre i comprovació que la informació ha estat veritablement guardada, caldrà fer proves de recuperació de les dades.

9. Xifratge de dades.

   Una altra mesura de protecció és xifrar les dades dels documents més confidencials, per la qual cosa, davant un robatori o còpia, ningú pugui accedir a les nostres dades.

10. Controlar que es fa amb les unitats USB i d'on provenen.

    Hem de controlar els orígens de les unitats d'emmagatzematge extern USB. Poden contenir malware. Hi ha casos d'USB que es troben al carrer que contenen un programa maligne. Si pensem que un USB és utilitzat en un equip infectat, hem de vigilar on el posem després.

11. Protegir documents, arxius i informació amb serveis en el núvol.

    És important utilitzar els serveis en el núvol com a contenidors de seguretat, tant en còpies de seguretat, com per a mantenir les nostres dades fora de l'abast dels ciberdelinqüents, normalment aquestes empreses inverteixen bastant en seguretat.

    És fonamental estar atents a les polítiques de privacitat. Sempre que utilitzem un servei desconegut hem de buscar opinions sobre aquest, tant en la seva fiabilitat i seguretat, com en l'accés que té el proveïdor d'aquest servei sobre les nostres dades.

12. Accedir només a xarxes de confiança WIFI.

Les xarxes WIFI obertes proliferen, però no són segures. Són el mitjà més senzill d'accedir als nostres dispositius. Recomanem accedir sempre a xarxes de confiança i amb seguretat activada per a garantir el xifratge de les dades que viatgen (VPN).

És important també que el dispositiu es desconnecti de les xarxes de comunicació després d'un període d'inactivitat, per a tancar la porta a possibles atacs.

13. Ús d'antivirus

Cal utilitzar proveïdor de confiança i repassar de tant en tant la capacitat d'aquests. En un mercat canviant les empreses apareixen, són comprades o es desfan en pocs mesos. Cal tenir sempre un antivirus de confiança i permanentment actualitzat.

Cal recordar que l'Antivirus del PC, no és el mateix que es posa en el servidor de correu, encara que aquest sigui Google o Microsoft. Aquestes empreses tenen els seus sistemes de seguretat, però si volem que sigui orientat a client, és a dir nosaltres, serà necessari afegir un Antivirus, Antispam, APT damunt dels servidors en qüestió per a tenir la màxima seguretat i evitar fins i tot que les empreses proveïdores de mail, puguin accedir al nostre mail.

14. Llocs d'accés WEB

Tot és suplantable, cal estar atents on ens connectem. Mirar les adreces web on anem, que siguin conegudes i de confiança. Cal desconfiar de les pàgines Web que no tenen HTTPS:// o el cadenat, sobretot si hem de fer transaccions on posem dades en el formulari. I mai connectar-se a pàgines de descàrregues il·legals que poden ser la nostra perdició. Vigilar les pàgines de continguts d'adults, d'ideologies alternatives o minoritàries, no sempre són el que diuen. Cal navegar en llibertat, contrastant i estar molt segurs d'on anem, i abans de donar dades preguntar als experts.

15. Phising

Desconfiar dels mails no esperats, d'adreces desconegudes o amb missatges màgics o de regals inesperats. Ningú regala res, ni en la vida, ni en Internet!! Els ciberdelinqüents exploten les nostres febleses humanes, ambició, diners, reconeixement, etc. Ni et donaran una herència llunyana, ni trobaràs l'amor desitjat, perquè t'han trobat per Facebook. Compte amb el que penges en les Xarxes Socials, que tens, on estàs, o la teva vida més íntima, a ningú li importa si et queda bé el vestit de bany de la temporada o si t'has canviat el cotxe, i menys on vius.

Mai donis dades bàsiques per mail, ni DNI, ni targetes de crèdit, ni números de compte, ni molt menys passwords. Si has d'enviar un número d'aquests, fes una part per mail i una altra per un altre mitjà, WhatsApp, Telegram o Signal, mai tot en un sol mitjà.

Comprova sempre que la direcció del remitent no conegut sigui creïble. En cas de dubte, consulta als experts.

El 90% dels atacs provenen del mail.

16. Firewall i VPN.

Internet és com un edifici ple de virus i bacteris. Com entraries? Protegit amb un vestit i tapat per tot arreu, veritat? Avui dia encara hi ha gent que es creu que pot accedir a Internet sense cap mesura de seguretat. L'accés ha de ser amb proteccions. L'ús del Firewall ens garanteix que el que entra, és bastant segur, i que el que surti, ho faci amb garanties que no es vagi el que no volem. Amb això ho tenim tot? No!! La ciberseguretat són capes, capes d'Antivirus, de Firewall, i de moltes coses més, però l'ús del Firewall està entre els bàsics per a treballar en aquesta xarxa amb seguretat. A més, ens permet crear les VPN privades quan estem fora del nostre (domini) despatx i accedir als recursos de l'empresa amb seguretat.

17. Monitoratge dels béns digitals.

Per què tenir un Firewall, si no ho usem?, per què tenir un cotxe, si està tancat en el garatge?

Els Firewalls i també els antivirus empresarials, tenen consoles de control que els gestors utilitzen per a analitzar el trànsit d'entrada i sortida de les nostres xarxes empresarials, on es poden detectar intents d'intrusió o sortida de material (digital) no desitjat. També el rendiment de les màquines i si han estat infectades per altres vies.

Si el nostre dispositiu va ralentitzat o ens dóna problemes, és convenient revisar l'ús de recursos que està utilitzant, mitjançant l'anàlisi d'aquests es pot detectar alguna amenaça de seguretat com un virus o una aplicació intrusiva que utilitza massa recursos.

Sense monitoratge, no es pot garantir la seguretat i encara menys l'origen dels problemes, si aquests es produeixen.

18. Habilitar l'accés remot i anotar el número IMEI dels mòbils.

En cas de pèrdua o robatori del nostre dispositiu, si tenim habilitat l'accés remot, podrem realitzar diverses accions, com pot ser conèixer la seva ubicació, bloquejar-ho o eliminar tot el contingut d'aquest.

Tant Android com iOS ens donen aquesta possibilitat i hem d'aprofitar-la. Si no tenim activat aquest accés, podem contactar amb el nostre proveïdor de telefonia i sol·licitar que ens bloquegi el dispositiu indicant el IMEI.

19. Reiniciar el dispositiu en rebutjar-lo.

    Sovint, quan canviem de terminal no acostumem a reiniciar de fàbrica el terminal antic. Per precaució, sempre és recomanable realitzar aquest reinici per a garantir la privacitat de la nostra informació.

20. Desconfiar i ser previngut.

    En els nostres dispositius rebem i consultem el correu i SMS, alguns d'aquests malintencionats. Davant el dubte, no obrim mai links que no tinguem a la seguretat que són de confiança, si tenim dubtes, contactem amb el remitent per a veure si realment ens ha enviat ell aquest correu o SMS.

    Denunciar el delicte o frau.

46329595M CARLES FLAMERICH (R: B66754847)

Firmado digitalmente por 46329595M CARLES FLAMERICH (R: B66754847)
Fecha: 2022.10.06 19:40:15 +02'00'

Carles Flamerich
CEO & CISO
C/ Sant Joan de La Salle 42 08022 BCN
T: +34 93 249 14 05 M: +34 638 684 928
carles.flamerich@light-eyes.com
light-eyes.com