>> Jorge Dávila

Confines BYOD: Hic sunt Dracones

Todo parece estar vitalizado por las modas y las tendencias, y el comportamiento humano frente a las tecnologías de la información no se ha salvado de ello. Parece que se pone de moda utilizar nuestros propios *gadgets* personales en nuestro trabajo y que ese uso continúa hasta mezclarse el ocio. Esta promiscuidad [1] que se llama BYOD requiere cierta atención, no vaya a ser que termine habitando entre nosotros.

Hace ocho siglos el mundo era pequeño. Los pueblos solo conocían aquellos lugares donde pudiesen llegar por sus pies, a caballo o donde el hambre les llevase. Superado el periodo de grandes migraciones en Europa (400-800 AD), se inicia la Edad Media y algunos estudiosos se dedican al confeccionar "*Mapas Mundi*" que resumían todo lo que del mundo sabían. En aquellas alegorías del mundo había confines, límites y vórtices donde el cartógrafo no sabía qué poner [2] y plasmaba su ignorancia con un gélido "*Terra ignota*". En algunos de esos tenebrosos lugares, distintos autores pintaron dragones, basiliscos, esfinges, serpientes, animales mitológicos y monstruosos para la cultura de los europeos de aquel entonces.

En una de esas representaciones, en el Globo de Hunt-Lenox [3] de 1503, uno de los globos terráqueos más antiguos que se conocen después del *Erdapfel* [4] de 1492, en su zona asiática aparece esa expresión latina de *Hic sunt Dracones*, "*aquí hay dragones*", con la que, desde entonces, se simboliza lo desconocido, el miedo que puede generar y la existencia de criaturas peligrosas que todavía no hemos visto y sufrido. La "Carta marina" de Olaus Magnus [5] (siglo XVI) es el mapa más antiguo de los países nórdicos y tiene una entrañable colección de esos monstruos nacidos del desconocimiento. La actual práctica conocida como BYOD recuerda a aquellas zonas ignotas en la que muy bien podría haber dragones.

"Bring Your Own Device" (BYOD), BYOT si nos referimos a la tecnología, o BYOP si concretamos en el teléfono móvil, se refiere a esa política empresarial que permite a los empleados llevar y utilizar sus propios artefactos móviles (portátiles, tabletas y *smartphones*) en su puesto de trabajo. Esas políticas incluyen permitir el acceso desde esos terminales a aplicaciones e informaciones (algunas de ellas privilegiadas) de la compañía.

La verdad es que, en muchos casos, los responsables de seguridad de las compañías no consiguen parar esa moda ya que, entre otros, los que más les presionan para permitirla son sus propios (altos) directivos. Los *gadgets* electrónicos son desde hace tiempo un símbolo de estatus social o empresarial, y ante esa presión sociológica de nada sirven los razonamientos o el sentido común.

El fenómeno BYOD comenzó en el año 2009, en las entrañas de Intel al aceptar esta empresa el creciente número de empleados que llevaban sus propios artefactos móviles al trabajo y los conectaba a la red telemática de la corporación. No dejó de ser en cierta manera una excentricidad más hasta que, a principios de 2011, ese término se hace popular de la mano de proveedores TI como Unisys, VMware o Citrix.

Las razones a favor de ese proceder podrían ser varias: (1) al ser los trabajadores dueños de los equipos de comunicación, se les puede localizar/controlar de forma más estrecha y aumentar así la productividad. (2) Al tener accesibles los asalariados más tiempo, la capacidad de respuesta frente a incidentes mejora sustancialmente y (3) al gestionar todos los intentos de conexión de equipos, el número de ellos que realmente están descontrolados disminuye considerablemente.

Los defensores del BYOD reconocen que con ello aumenta el riesgo de que los empleados se lleven datos sensibles en sus equipos móviles, pero afirman que las organizaciones pueden manejar dichos riesgos suplementarios. Esta tendencia nace de la creencia resignada de que no se puede no hacer nada dado que los empleados terminaran encontrando el modo de conectarse con sus equipos y, de hacerlo sin control, estarían poniendo en grave riesgo a la empresa.

El poder de seducción de la extravagancia BYOD está en que sus apóstoles dicen que los empleados terminan siendo más productivos, ya que el hecho de que usen su propia tableta o *smartphone* hace atractiva a la empresa y su trabajo en ella. Además, los empleados cuidan de los equipos ya que son suyos y, como se trata de una moda, las empresas se benefician de un cambio tecnológico más rápido y acceden a lo último en tecnología de forma más rápida. Por si fuera poco y para mayor complacencia del trabajador, son ellos los que deciden qué tecnología y marca utilizar. Lo más atractivo

El atractivo de estos equipos, basta con explotar las inmadureces y debilidades de los jóvenes sistemas operativos que corren en ellos, se basa en la la prolija variedad de modos de comunicación que atienden (voz, datos, mensajería, posición, trayectos, navegación, correo, etc.); y en la innumerable colección de aplicaciones de todo tipo que se instalan en ellos, que rara vez han sido seriamente estudiadas en cuanto a su seguridad, origen y verdaderas funcionalidades.

[1] Promiscuidad en su segunda acepción "*Mezcla desordenada de elementos* [usos] *diversos*".

[2] "*Como geógrafo, Sosio, abarrotaba los bordes de sus mapas del mundo que conocemos, añadiendo notas en los límites indicando que más allá de esas líneas no se encuentran nada más que desiertos llenos de arena, bestias salvajes y ciénagas inaccesibles*". Plutarco (46-120 dC) en "*La vida de Teseo*".

[3] Ver http://exhibitions.nypl.org/treasures/items/show/163

[4] El *Erdapfel* (manzana de la tierra en alemán) construido por Martin Behaim en 1492 es el globo terráqueo superviviente más antiguo. El mapa fue pintado por Georg Glockendon y está albergado en la Rare Book Division de la Biblioteca Pública de Nueva York. De él resulta chocante la clara ausencia de América http://en.wikipedia.org/wiki/File:MartinBehaim1492.png

[5] Ver http://en.wikipedia.org/wiki/Carta_marina

para la empresa es que se libra de pagar la parte bastante cara de los instrumentos con los que trabajan sus asalariados.

En contra tenemos, al menos, que (1) la información de la compañía está menos segura que si se mantiene en equipos propiedad de la empresa, (2) que el esfuerzo administrativo (personas y equipos) para la gestión de ese hardware no sólo no disminuye, si no que puede ser mayor dada la heterogeneidad que llevan asociadas las políticas BYOD. (3) En aras a la seguridad, los empleados terminan perdiendo el control total de sus equipos, ya que la empresa querrá asegurarse de que su información privada y confidencial realmente está segura. (4) Los empleados pagan sus propias herramientas y, en muchos casos, son los responsables de arreglarlas cuando se estropean o se rompen.

A pesar de todo lo anterior no se habla con suficiente claridad de los riesgos que entraña llevar los límites de la empresa hasta confines tan poco explorados como son esos "*Own Devices*"; verdaderas tierras ignotas del siglo XXI.

BYOD es un ejemplo de lo que se conoce como el "*end node problem*"[6] o "*problema de seguridad en el punto final*". En este escenario, ordenadores individuales se utilizan en trabajos sensibles y, temporal o permanentemente, pasan a formar parte de una red confiable y bien gestionada. Más tarde, esos mismos equipos son utilizados en actividades más arriesgadas o se conectan a redes no confiables.

La seguridad de los equipos móviles es uno de los frentes más arriesgados que presenta el escenario actual. Aunque los casos ya conocidos se centran más en la pérdida de datos personales, eso no quiere decir que no ocurra otro tanto aún mayor con los datos empresariales.

El problema nace de querer utilizar una única herramienta para todas las comunicaciones y para planificar todas las actividades, sin distinguir si son profesionales o de la vida privada. Tal concentración de información hace muy atractivos esos equipos como objetivos de ataque. Así, basta con explotar (1) las inmadureces y debilidades de los jóvenes sistemas operativos que corren en ellos, (2) la prolija variedad de modos de comunicación que atienden (voz, datos, mensajería, posición, trayectos, navegación, correo, etc.), (3) la innumerable colección de aplicaciones de todo tipo que se instalan en ellos y que rara vez han sido seriamente estudiadas en cuanto a su seguridad, origen y verdaderas funcionalidades se refiere.

Se están incluyendo contramedidas para tratar de paliar los efectos de ese descontrol, fundamentalmente el estratificado y compartimentalización del software que se ejecuta pero claramente están resultando insuficientes y, en algunos casos, del todo inútiles.

Los usuarios BYOD están expuestos a varias amenazas que alteran el comportamiento de sus equipos y transmiten o modifican datos del usuario. Las aplicaciones que se ejecutan no pueden garantizar la intimidad y la integridad de la información que manejan, si no lo hace antes el sistema operativo que la ejecuta. Además de eso, en el escenario BYOD es donde más sentido tiene el paradigma de los caballos de Troya, puesto que es el propio usuario el que se instala el *malware* (sin saberlo) y le otorga potestades prácticamente plenipotenciarias.

El botín perseguido son los datos, (números de tarjetas, información de autenticación, información privada, registro de actividad, calendarios, listas de llamadas, agenda, recorridos GPS, etc.). También es muy jugoso el negocio de la obtención de identidades y la posibilidad de bloquear la disponibilidad atacando el equipo en el que el usuario "lo tiene todo".

Los atacantes, son los de siempre: los *hackers* profesionales, civiles o militares, que roban información sensible de la gente, que se afanan en el espionaje industrial o que utilizan a sus víctimas como tapaderas para ataques de mayor altura. También están en este negocio los ladrones que quieren obtener dinero a través o a cambio de los datos personales o corporativos que puedan sustraer. No hay que olvidar a los diseñadores y diseminadores de *malware* que esencialmente pretenden atacar a la disponibilidad de los datos y servicios que proporcionan esos equipos móviles.

El atacante puede manipular el equipo móvil y convertirlo en un zombi a su servicio que puede (1) hacer llamadas, (2) grabar conversaciones al mejor estilo de florero puesto en una mesa con comensales interesantes, (3) que puede suplantarnos ante todas las redes en las que nos dejen entrar y nos concedan algún crédito, (4) que puede agotar en poco tiempo la batería, o (5) borrar ciertos registros que lobotomiza irreversiblemente al teléfono inteligente convirtiéndolo en un simple ladrillo.

El verdadero problema del BYOD es (1) la inmadurez de los sistemas operativos que se utilizan, (2) lo silvestre de las aplicaciones que se suelen instalar, (3) la falta de mesura a la hora de entregarles potestades y, sobre todo, (4) la arriesgada concentración de información en un solo dispositivo o en un reducido número de ellos.

Hace ya 166 años, el médico húngaro Ignaz Semmelweis demostró que con el mero hecho de lavarse las manos con una solución fenólica o con lejía diluida, disminuía el número de fiebres puerperales, una forma muy seria de septicemia que, en aquellos tiempos, se llevaba por delante a más del 10% de las madres[7].

Ahora parece normal mantener un mínimo de higiene, pero este instinto aséptico no ha estado siempre con nosotros.

El verdadero problema del BYOD es la inmadurez de los sistemas operativos que se utilizan, lo silvestre de las aplicaciones que se suelen instalar, la falta de mesura a la hora de entregarles potestades y, sobre todo, la arriesgada concentración de información en un solo dispositivo o en un reducido número de ellos.

No concentrar en uno o unos pocos instrumentos informáticos móviles toda nuestra vida y todo nuestro trabajo es algo que aconseja el sentido común. No mezclar tres ámbitos que necesariamente no tienen nada que ver entre sí (trabajo, vida privada y ocio) es la primera medida profiláctica que nos puede llevar a cotas de seguridad informática hoy no alcanzadas.

Las observaciones de Semmelweis no gustaron a la clase médica consolidada y sus ideas fueron rechazadas por la comunidad de doctores hasta que más tarde las confirmó Louis Pasteur. Las recomendaciones de Semmelweis sólo fueron ampliamente aceptadas pasados varios años después de su muerte, a los 47 años, en un manicomio vienés y por una paliza que le propinaron sus guardianes.

En los confines de la cadena, en el limbo de nuestros sistemas informáticos, en los terrenos ignotos de nuestros terminales móviles es donde hoy hay dragones. ■

Jorge Dávila Muro
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es

[6] Ver http://en.wikipedia.org/wiki/End_node_problem

[7] "*Only the clinical facts proved him right during his lifetime; the triumph of bacteriology which began after his death made him not only the 'savior of mothers' but also a genial ancestor of bacteriology*" en Hanninen O, Farago M, Monos E.: "*Ignaz Philipp Semmelweis, the prophet of bacteriology*", Infect Control 4(5) Sep-Oct, pags. 367-370, 1983.