¿POR QUÉ ES IMPORTANTE LA SEGURIDAD EN CAPAS?

Firewall

Antivirus

Defensa proactiva frente al malware

Desinfección

Educación del usuario

¿QUÉ ES LA SEGURIDAD EN CAPAS?

Es la utilización de una combinación de varias soluciones de ciberseguridad para reducir los puntos vulnerables de un sistema conectado en red.

¿CUÁLES SON LOS DESAFÍOS MÁS RECIENTES?

La mayoría de los administradores de TI y profesionales de la seguridad opinan que hay un aumento significativo del riesgo en los terminales debido a:

73 % uso de aplicaciones comerciales en la nube

63 % empleados que trabajan desde casa o desde ubicaciones exteriores

68 % dispositivos móviles propiedad de los empleados

INFRACTORES MÁS HABITUALES

Ataques de malware experimentados por redes de TI durante el último año (se permiten varias respuestas):

- **80 %** Ataques de malware originados en la web
- **65 %** APT/ataques dirigidos.
- **65 %** Rootkits
- **55 %** Ataques intensos de phishing

AUMENTO DE LA GRAVEDAD Y LA EFICACIA

69 % de los que respondieron afirmaron que la gravedad de los incidentes de malware ha aumentado en el último año.

60 % de las veces, los atacantes son capaces de poner en peligro toda una organización en cuestión de minutos[1].

¿DÓNDE SE ENCUENTRAN LOS PUNTOS DÉBILES DE SUS DEFENSAS?

NO ESTÁ AL DÍA

De los 7 millones de vulnerabilidades de seguridad conocidas públicamente, solo **10 suponían casi el 97 %** de los exploits observados en 2014[2].

El **99,9 %** de las vulnerabilidades explotadas seguían en situación de riesgo **más de un año** después de su publicación.

SEGURIDAD DÉBIL

Tiempos de detección

demasiado prolongados,

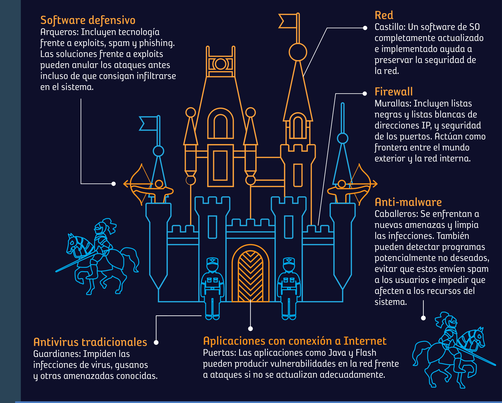
errores conocidos no solucionados, directivas de seguridad no aplicadas, o una codificación **conocida, inexistente o implementada** incorrectamente, falta de protección frente al malware, configuraciones inalámbricas vulnerables, problemas físicos de seguridad, información desestructurada, aplicaciones antiguas que ya no reciben asistencia, proveedores y socios no protegidos por completo.

USUARIOS NEGLIGENTES O MAL INFORMADOS

- Caen en los ataques de phishing y otras tácticas de ingeniería social.
- Intentan burlar las medidas de seguridad e instalan malware directamente en el sistema.
- Proporcionan credenciales durante los ataques de phishing.
- Publican información de seguridad en redes sociales.

¿QUÉ CAPAS NECESITA?

Soluciones tecnológicas



Software defensivo
Arqueros: Incluyen tecnología frente a exploits, spam y phishing. Las soluciones frente a exploits pueden anular los ataques antes incluso de que consigan infiltrarse en el sistema.

Red
Castillo: Un software de SO completamente actualizado e implementado ayuda a preservar la seguridad de la red.

Firewall
Murallas: Incluyen listas negras y listas blancas de direcciones IP, y seguridad de los puertos. Actúan como frontera entre el mundo exterior y la red interna.

Anti-malware
Caballeros: Se enfrentan a nuevas amenazas y limpia las infecciones. También pueden detectar programas potencialmente no deseados, evitar que estos envíen spam a los usuarios e impedir que afecten a los recursos del sistema.

Antivirus tradicionales
Guardianes: Impiden las infecciones de virus, gusanos y otras amenazadas conocidas.

Aplicaciones con conexión a Internet
Puertas: Las aplicaciones como Java y Flash pueden producir vulnerabilidades en la red frente a ataques si no se actualizan adecuadamente.

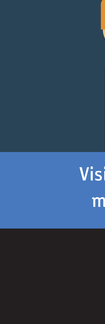
Soluciones de sensibilización

¿Están documentadas?

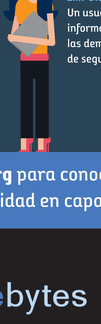
¿Son estas razonables?

¿Siguen los empleados realmente las directivas de seguridad?

¿Cuento con la ayuda de la tecnología para aplicar estas directivas?



El administrador de TI recopila conocimientos sobre amenazas a partir de fuentes externas y los usa para repeler los ataques y mantiene protegidos a los usuarios con directivas eficaces.



El usuario constituye **LA MEDIDA DE SEGURIDAD MÁS IMPORTANTE**. Un usuario bien informado refuerza las demás capas de seguridad.

Visite **www.malwarebytes.org** para conocer más detalles sobre la seguridad en capas

Malwarebytes

Fuentes:
1. 2015 State of the Endpoint Report: User- Centric Risk. (2015, Informe sobre el estado del terminal, riesgos centrados en el usuario), patrocinado por Lumension, realizado de forma independiente por Ponemon Institute LLC (enero de 2015); Verizon 2015 Data Breach Investigations Report (Informe de investigación sobre vulnerabilidades de datos de Verizon en 2015)
2. Verizon 2015 Data Breach Investigations Report (Informe de investigación sobre vulnerabilidades de datos de Verizon en 2015)