Dispositivos SmartKeeper

Seguridad en Redes

Agenda

- Propuesta de Valor
- Cibercrimen
- Protocolo de Seguridad
- Resumen del Producto
- Competencia

Propuesta de Valor:

- El producto de seguridad física SmartKeeper ofrece un mecanismo de bloqueo único para evitar el acceso no autorizado a los puertos abiertos, agregando una capa de seguridad física al sistema ya implementado. Una llave maestra controla varios dispositivos para bloquear una variedad de puertos, lo que reduce el riesgo de daños intencionales o no intencionales, ahorrando tiempo y dinero asociado con violaciones de datos, tiempos muertos de la red y reparación de la infraestructura.

¿Suena familiar?

Twitter
330M de registros
Un error almacenó contraseñas en texto legible.

WorldPress
76.5M de registros
Vulnerabilidad de Seguridad

Facebook
29M de registros
Información de perfil recopilada por terceros maliciosos

Uber
57M de registros
Uber pagó a los hackers 100.000 dólares para eliminar datos robados.

Quora
100M de registros
Accesos comprometidos

MyHeritage
92.2M de registros

British Airways
380k de registros
Los datos personales y financieros de clientes se vieron comprometidos

Orbitz
880K de registros
Información de Tarjetas de Pago

T-Mobile
2M de registros

Marriott Hotels
383M de registros
Datos sensibles filtrados desde 2014

Blur
2.4M de registros

Amazon
100k de registros
Nombres de clientes y direcciones de correo electrónico divulgados accidentalmente en su sitio web.

Google
52.5M de registros
Los datos personales de usuarios podrían haber quedado expuestos.

Violaciones de datos…..”la nueva normalidad”

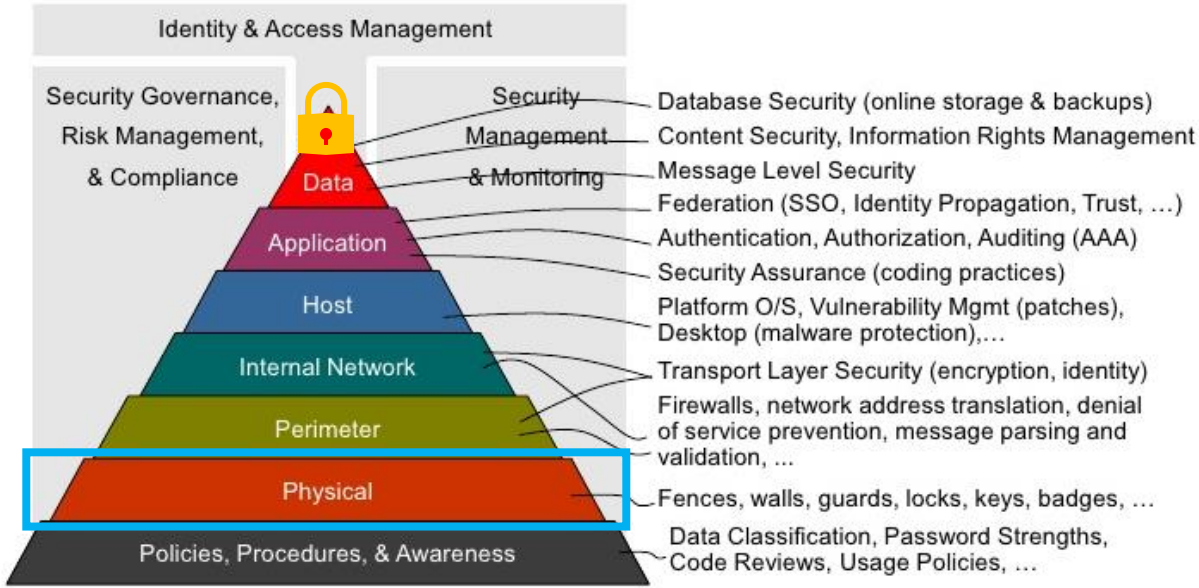
- Los riesgos de ciberseguridad están incrementando debido a la creciente dependencia en los sistemas informáticos y dispositivos inteligentes.
- Se estima que para el 2020 hayan cerca de 200 mil millones de dispositivos conectados.
- El 95% de las violaciones se deben a errores humanos.
- El costo promedio de una violación de datos en 2020 excederá los $150M USD.
- Un puerto abierto es una invitación a acceder fácilmente a sus datos... Bloquéelos!
  - El sector empresarial tuvo la mayor cantidad de violaciones de datos en 2018
  - El sector de la salud, tuvo la segunda mayor cantidad de violaciones en 2018

“El cibercrimen es la mayor amenaza para toda empresa en el mundo”

Ginni Rometty, presidente, director y CEO de IBM

Objetivos principales…

Proteja sus datos, añada capas a su seguridad



Ejemplos de algunas violaciones de seguridad:

College of St Rose en Nueva York, un ex alumno usó una memoria USB como arma llamada "USB Killer" (“USB asesina”) que compró en línea para destruir 59 computadoras, 7 monitores de computadora y podios mejorados para computadora que tenían puertos USB abiertos. 14 de febrero de 2019.

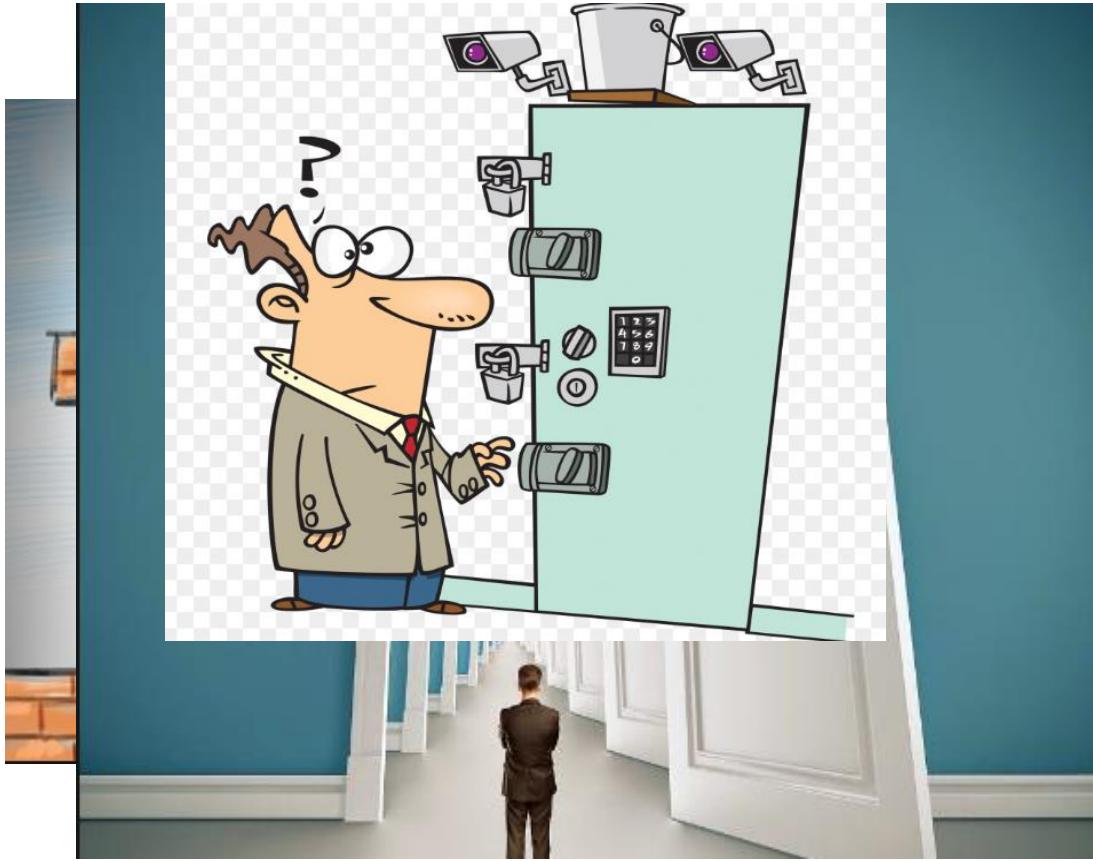
Marriott Hotels, reconocieron que una parte no autorizada había copiado y encriptado información perteneciente a los clientes en su sistema de reservas Starwood. Accediendo así a información de pasaportes y detalles de tarjetas de crédito desde 2014. Después de seguir una investigación, se estimó que el tamaño del hackeo ronda los 383 millones. Noviembre de 2018.

Google, descubrió un virus en las API de Google+ durante su procedimiento de pruebas habitual. Esta es la segunda vez que sucede, afectando a 52,5 millones de usuarios. Este sitio se cerró en abril de 2019 después de ser descubierto en noviembre de 2018.

Toyota, se detectó acceso no autorizado en los sistemas informáticos de varias subsidiarias de ventas de Toyota y Lexus en Tokio, lo que filtró información de aproximadamente 3,1 millones de clientes. Febrero de 2019.

¡No lo haga fácil!

- Cree múltiples obstáculos
  - No dependa solo del software
- No deje ninguna puerta abierta
  - Un puerto abierto es un potencial acceso a sus datos
- ‘Cierre y asegure la entrada’
  - Bloquee los puertos que llevan a sus datos



Panduit puede ayudarle…

- Nueva línea de dispositivos de bloqueo de seguridad de redes con mecanismo de llave única

SKMKEY

UNA LLAVE
Múltiples dispositivos

SKUSBA-V

SKUSBC

SKRJ45RD-X

Dispositivo de bloqueo USB tipo A SKUSBA-V

- La USB es una interfaz popular *plug and play* que permite a las computadoras comunicarse con otros dispositivos. También es una forma fácil de transferir malware o dañar equipos.

- Compatible con los puertos Tipo A que se encuentran comúnmente en la mayoría de los dispositivos host
- Se monta al ras con el puerto
- Fácil instalación con un solo movimiento
- Extraíble con la llave maestra SmartKeeper de Panduit
- Reemplazará la oferta existente de PSL-USBA

Dispositivos de bloqueo USB Tipo C

- Ampliamente adaptado desde 2015, se espera que su uso aumente al reemplazar varios tipos de conexiones que permiten que las computadoras se comuniquen con otros dispositivos, lo que hace que sea un punto de fácil acceso a los datos.

- Compatible con puertos Tipo C que se encuentran en una variedad de dispositivos periféricos y host
- Mecanismo de bloqueo fácil de un solo movimiento después de insertarse en el puerto
- Extraíble con la llave maestra SmartKeeper de Panduit

Dispositivos de bloqueo RJ45

- Los puertos RJ45 se encuentran en casi cualquier dispositivo, proporcionando acceso a la red y sus datos. El puerto también puede resultar dañado por un objeto externo.

Bloqueado

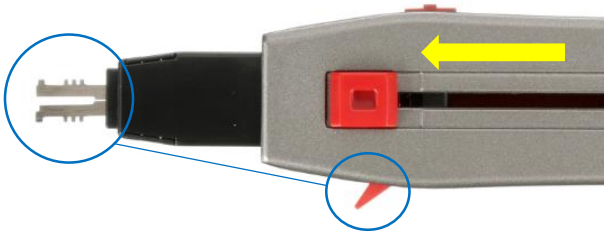
Desbloqueado

- Compatible con la mayoría de las aperturas RJ45
- Disponible en color rojo
- Mecanismo de bloqueo fácil de un solo empuje después de insertarse en el puerto
- Extraíble con la llave maestra SmartKeeper de Panduit

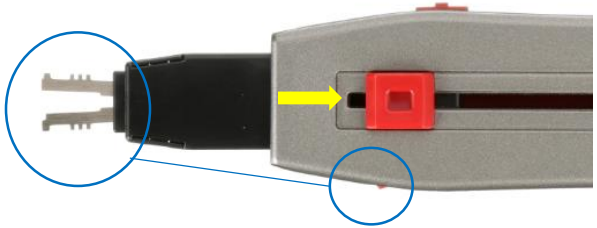
Llave maestra SmartKeeper

- El patrón de la cuchilla es único y solo compatible con los dispositivos de bloqueo SmartKeeper de Panduit
- El botón deslizante expulsa o retrae las cuchillas con llave; bloquea las cuchillas en el dispositivo para su extracción
- La palanca lateral también bloquea la llave en el dispositivo cuando se presiona
- Incluye luz que se activa con un interruptor
- Con empuñadura de goma antiestática

Llave maestra – etapas funcionales



Desbloqueada – (cuchillas están muy juntas) Se usa para insertar o quitar del dispositivo



Bloqueada - (cuchillas abiertas) Se usa para sacar el dispositivo del puerto

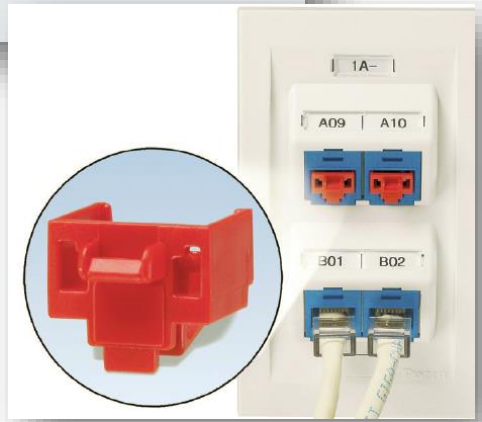
Vista interna cuando está bloqueada
Lista para extraerse

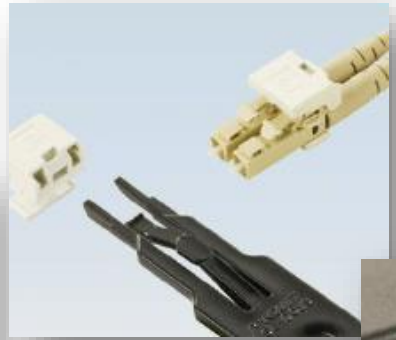
Recuerde….

- Una interfaz *plug and play* común permite que las computadoras se comuniquen con otros dispositivos
- No tiene que ser un dispositivo convencional
- Tener un puerto abierto es como darle las llaves de su casa a un extraño
- Cierre todo acceso abierto a sus datos con los dispositivos de seguridad de redes SmartKeeper de Panduit.

Productos de Seguridad Física Adicionales…

- Panduit ofrece una amplia oferta de dispositivos de seguridad para satisfacer la mayoría de las necesidades.





Gracias…