LA CIBERSEGURIDAD EN LAS PYMES

Herve Lambert – Global Consumer Operations Manager

Oliver Lecerf – Global Consumer Business Development Manager

El poder de la tecnología en las PYMES

Cómo la tecnología puede mejorar la productividad de tu negocio

10 Claves tecnológicas para mejorar la productividad de las empresas

1. Trabajar en micro-proyectos con pequeñas inversiones tecnológicas generando impacto en los **modelos de negocio.**

2. Mejorar motivación del equipo, integrar **automatización** de procesos manuales.

3. Control de **niveles de productividad** por persona ocupada.

4. Gestionar la **seguridad** de la empresa con capacitaciones y generar una cultura de seguridad informática.

5. **Reducir** los costos de gestión, utilizando recursos internos para proyectos de innovación en la empresa y el mercado.

10 Claves tecnológicas para mejorar la productividad de las empresas

6. **Ingeniería humanista**.. Aplica la tecnología desde un punto de vista más humano.

7. **Apostar por el conocimiento, por los bienes y equipos de trabajo** que requieran poca inversión.

8. Poner el foco en la **innovación tecnológica y proyectos con retorno rápido**.

9. **Reeducar la gerencia** sobre la importancia de las inversiones en innovación y tecnología.

10. Generar **inteligencia compartida** y espíritu innovador del equipo.

Ciberseguridad: ¿Algo más que protección?

Datos básicos desde Panda Security sobre el malware

Cuanto mayor sea el **nivel de digitalización** de una empresa, mayor será la **vulnerabilidad de sus sistemas**. El **delito cibernético cuesta al mundo 575.000 millones de dólares al año**, lo que representa el **0,8% del PIB mundial**.

Según Pandalabs:

20% **de las infecciones** de malware en Latinoamérica **se difunden a través de USBs o tarjetas SD**.

75M de **ficheros de malware distintos** se detectaron **en 2018** (285.000 nuevos ejemplares de malware día).

99% del malware ha sido visto una única vez en un año: crece el **malware especifico para hacer ataques dirigidos**.

80% de todos los ciberataques en empresas están relacionados con **vulnerabilidades conocidas** que no están siendo parcheadas en el momento adecuado.

Datos básicos desde Panda Security sobre el malware

Según Pandalabs:

86% de las **vulnerabilidades** provienen de **software de terceros**, no del sistema operativo.

4,5% de las **pequeñas empresas sufren infecciones** en México.

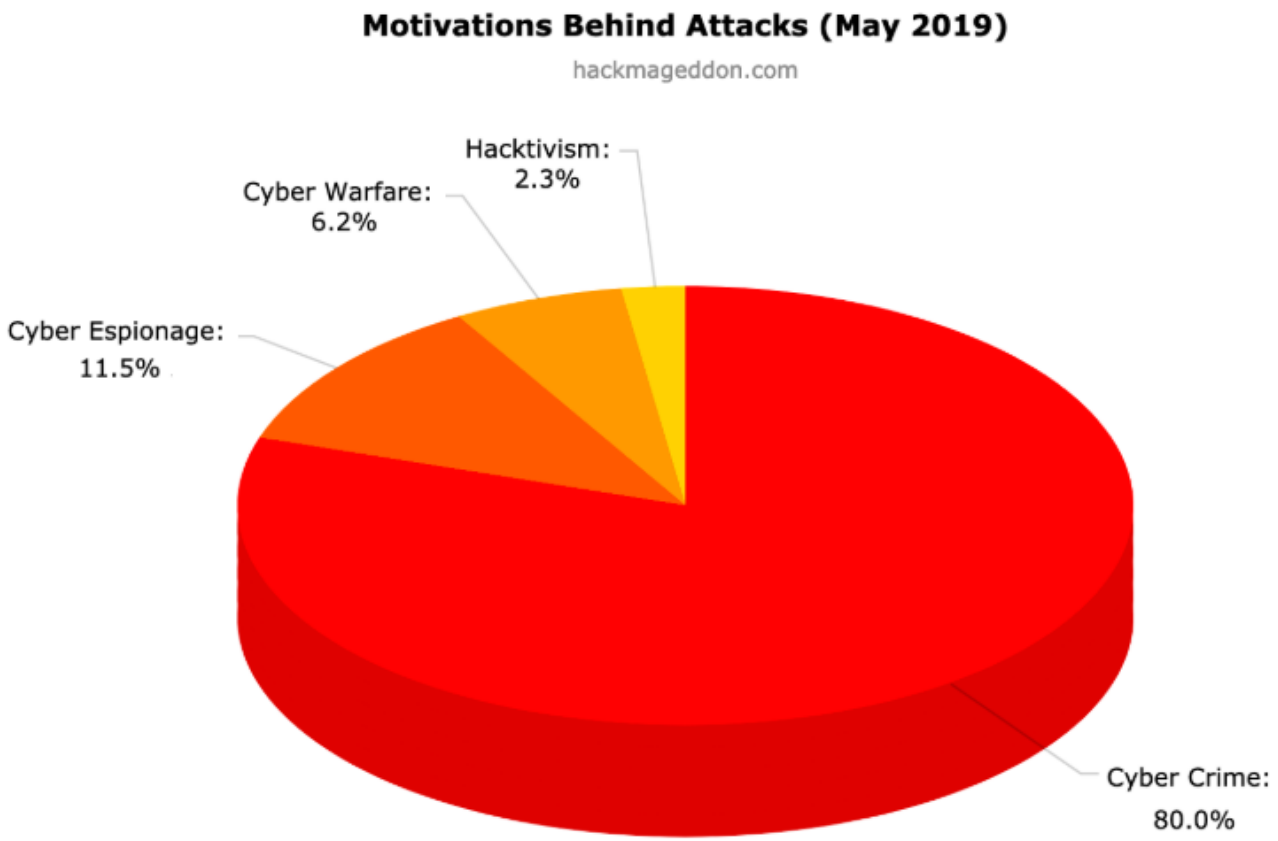
2 de **5** **organizaciones sufre brechas de seguridad** provocadas por malware.

80% de los ataques empiezan con **ataques de phishing.**

3,5 veces más que el mismo periodo del año pasado ha sido el **crecimiento de la minería de criptomonedas.**

Motivaciones de los malos: ¿qué buscan?

Los tipos de datos más valiosos para los ciberdelincuentes



- Dinero
- Información del cliente/empresa
- Información financiera
- Planes estratégicos
- Información del Consejo
- Contraseñas del cliente
- Información de I&D
- Datos de fusiones/adquisiciones
- Propiedad intelectual
- IP no patentada
- Información de proveedores

No será fácil proteger la PYME.. ¿le resulta familiar?

6,4 Billones de correos falsos

Fueron enviados alrededor del mundo cada día en 2018.

Fuente: Dark Reading, Agosto 2018

1.464 Funcionarios del gobierno

De un estado en los EE.UU. utilizando "Password123" como contraseña.

Fuente: The Washington Post, Agosto 2018

2 Billones De registros personales

Y otros datos sensibles fueron comprometidos entre enero 2017 y marzo 2018.

Fuente: Chronology of Data Breaches, Marzo 2018

550 Millones

De emails de phishing enviados por una sola compaña en el primer trimestre del 2018

Fuente: Dark Reading, Abril 2018

5.750 Empresas

Empresas son atacadas al día en México.

Fuente: PandaLabs- Panda Security

50% Autoridades locales

En Inglaterra dependen de un software en un servidor sin soporte.

Fuente:Computing, Agosto 2018

2 Millones de identidades

Robadas se usaron para realizar comentarios falsos en una encuesta de los EE.UU.

Fuente:4 Naked Security, Mayo 2018

10.000 Ordenadores bloqueados

Con un virus en el ayuntamiento de Baltimore. Los atacantes exigían 100,000 US$ para terminar el bloqueo.

Fuente: elpais.com

US$ 3.62 Millones

Costó de promedio una filtración de datos en el 2018 en EE.UU.

Fuente: Ponemon Institute, Julio 2017

74% Internautas

Se conecta en cualquier sitio desde su diapositiva móvil.

Fuente: Asociación de Internet de Mexico

Las vulnerabilidades

- Empleados descuidados o inconscientes
- Sistemas de seguridad obsoletos o inadecuados
- Vulnerabilidades en el software
- Acceso no autorizado
- La computación en la nube
- Los smartphones / tablets
- Las redes sociales
- Internet de las cosas

Entonces, ¿Cómo afrontamos esta situación?

12 recomendaciones de seguridad para proteger a la PYME

1. Almacena los datos en los **recursos de la empresa** (no en dispositivos personales).

2. **Cifra la información que intercambias** con clientes / proveedores (por ejemplo: comprimir fichero con contraseña).

3. Atención al usar USBs : **cifra los datos** en caso de pérdida del USB.

4. Si usas disco duro externo, solicita que se hagan **copias de seguridad.**

5. Al eliminar un dispositivo (PC, disco externo , etc.) realiza un **borrado seguro de los datos**.

6. Al eliminar **documentos físicos** utiliza la **destructora de papel.**

12 recomendaciones de seguridad para proteger a la PYME

7. Utiliza **contraseñas robustas** ➔ pásate a la **passfrase**

Cómo pasarse al PASSFRASE

Conceptos clave:

- **No uses información personal**.
- Utiliza **caracteres especiales, mayúsculas, minúsculas y números**.
- Recuerda que para que sea difícil de descifrar, es importante **que sea larga (más de 16 caracteres**).
- Asegúrate que sea **fácil de recordar (para ti).**

Ejemplo de PassFrase:

1. Piensa en una frase fácil de recordar, que NO contenga datos personales tuyos. Ejemplo: **Me gusta el cine mudo**
2. Une las palabras y pon la inicial de cada palabra en mayúsculas: **MeGustaElCineMudo**
3. Puedes añadir un carácter especial como el símbolo # y un número y colocarlos en un sitio fácil de recordar (inicio o final). Por ejemplo: **#MeGustaElCineMudo2**

12 recomendaciones de seguridad para proteger a la PYME

8. **Bloquea tu equipo** al ausentarte de tu puesto de trabajo.

9. No dejes papeles con **información confidencial** en tu mesa.

10. Cuando te desplaces **vigila tu computadora, tablet o teléfono**. Se recomienda **cifrar los datos** de los discos duros.

11. **Evita conectarte a redes Wi-Fi de lugares públicos** (hoteles, restaurantes, etc.) con dispositivos del trabajo. Si tienes que mandar datos confidenciales **usa una VPN.**

12. **Sentido común:** si tienes dudas pregunta a tu asesor tecnológico.

MUCHAS GRACIAS

panda

pandasecurity.com