Ciberseguridad

¿Cómo incorporarla en la PyME?

Ana Lucero
Joaquín Pérez

Agenda

1. ¿Por qué estamos aquí?
2. Tres ideas...¿ciertas?
3. ¿Por qué proteger mi empresa si...?
4. Tipos de ataques exitosos
5. ...¿y en Uruguay qué sucede?
6. Incidentes de ciberseguridad 2016 Uruguay (reportados)
7. ¿Por qué proteger las PyME?
8. Consejos para proteger las PyME
9. Medidas de bajo costo y alto impacto

¿Por qué estamos aquí?

Seguridad de la información
Planificación
Documentación
Control de acceso
Procedimientos operativos
Antivirus y antimalware
Penetration testing
Procesos críticos de negocio
Acuerdos de nivel de servicio
Monitoreo de infraestructura y eventos
Ethical hacking
Procedimientos de gestión
Desarrollo seguro
Seguridad física y ambiental
Evaluación de vulnerabilidades
Riesgos
Inventario de activos
Relacionamiento con terceros
Ciberseguridad
Respaldos
Políticas
Gestión humana y concientización
Firewalls y segmentación
No divulgación
Cumplimiento normativo

Tres ideas... ¿ciertas?

- La ciberseguridad es molesta
- La ciberseguridad es cara
- La ciberseguridad solo involucra a TI y no al negocio

¿Por qué proteger mi empresa? Si:

En Uruguay nunca pasa nada

No tengo presupuesto para seguridad

Es un problema de TI, lo resuelven ellos

Nunca me enteré de incidentes en mi empresa

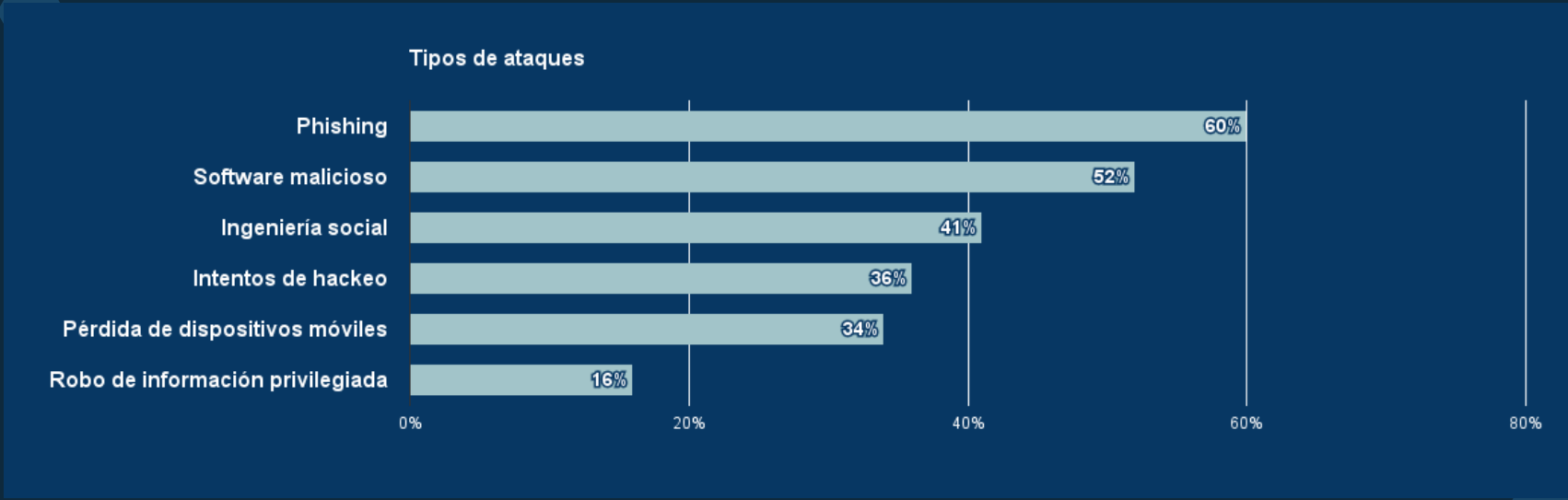
A nadie le interesa robar mi información

A mí no me va a pasar nada

La torta alcanza para todos

¡Nadie está libre! Veamos...

Tipos de ataques exitosos (EEUU & Europa)



Los principales tipos de ataque están relacionados con las personas

Fuente: State of Cybersecurity – Implications for 2016 – An ISACA and RSA Conference survey

...¿y en Uruguay qué sucede?

HACKERS ENCRIPTARON ARCHIVOS Y UTILIZARON LÍNEAS TELEFÓNICAS DE 5 EMPRESAS

La mafia nigeriana secuestra datos de empresas uruguayas

ATAQUES INFORMÁTICOS

Advierten por virus informático que llega como falso mail de la DGI

TECNOLOGÍA

Advierten aumento de ataques ínformáticos por WhatsApp

BPS - Empresas afectadas por el tornado de Dolores

La Resolución de Directorio del BPS Nº 10-35/2016 del BPS estableció diversas medidas tendientes a contemplar la situación de las empresas que se vieron afectadas por el tornado de la ciudad de Dolores.

Incidentes de ciberseguridad 2016 Uruguay (reportados)

419

Incidentes de ciberseguridad reportados en el 1er semestre de 2016

377

Incidentes de ciberseguridad reportados en el 1er semestre de 2015

11%

De aumento en 2016 respecto al mismo período en 2015

Fuente: cert.uy
Comunidad objetivo: Organismos estatales, no incluye al sector privado

¿Por qué proteger las PyME?

ECONOMÍA Y EMPRESAS INFORME

Seguridad de la información: un desafío para las pymes

En Uruguay todavía falta concientización sobre la importancia de cuidar los datos y políticas empresariales para evitar ciberataques

AMPLIANDO EL MERCADO

Nuevo régimen para que las Pymes se financien en bolsa

28 Abr Jornada: Factores de competitividad para una internacionalización exitosa de las PYMEs (26 mayo)

Conceptos como diplomacia corporativa y lobby, due diligence reputacional, legal compliance o ciberseguridad serán protagonistas en esta jornada.

La falta de ciberseguridad frena al inversor a la hora de apostar por una compañía

¿Por qué proteger las PyME?

- Mayor presencia en Internet
- Posibilidad de encontrar información atractiva como ser datos personales, números de tarjetas de crédito, etc.
- En general, se destinan menos recursos para seguridad que las grandes empresas
- Como consecuencia, se requeriría menos esfuerzo para vulnerar sus medidas de seguridad

¿Por qué proteger las PyME?

- Valor de la PyME
- Búsqueda de inversiones
- Consecuencias legales, económicas y reputacionales.
- La ciberseguridad no es solamente un tema del personal de TI, es un vehículo para generar confianza en las relaciones comerciales.

Consejos para proteger la PyME

Política de Seguridad de la Información

PERSONAS

Compromiso de la Dirección

Actividades de sensibilización y capacitación

PERSONAS

Acuerdos de no divulgación

Referente de seguridad de la información

PROCESOS

Procesos y activos críticos

Riesgos

Impacto en el negocio

PROCESOS

Controles

Respuesta a incidentes

Continuidad

Recuperación

TECNOLOGÍA

Firewalls, segmentación

Software y hardware actualizado

Medidas de seguridad en PCs

TECNOLOGÍA

Cifrado de pendrives y discos duros

Antivirus-Antispyware

Monitoreo

Medidas de bajo costo y alto impacto para incorporar ciberseguridad en la PyME

Personas

COMPROMISO

- Dirección comprometida
- Difusión y concientización: afiches, charlas, comunicados, etc.
- Acuerdos de no divulgación en las relaciones laborales y con terceros
- Escritorios limpios
- Bloquear la sesión de los PCs al retirarse del escritorio
- No anotar ni compartir contraseñas (ni siquiera con proveedores de servicios informáticos)

COMUNICACIÓN

- No registrar la dirección de correo electrónico laboral en sitios web
- Destrucción segura de documentos, CDs, DVDs, etc.
- Involucrar a los colaboradores y recordarles que la seguridad es tarea de todos
- Capacitar en el uso adecuado de las redes sociales corporativas y personales
- No abrir correos de remitentes desconocidos o mensajes sospechosos

CAPACITACIÓN

- No utilizar correos personales para usos laborales. Utilizar el correo empresarial únicamente para fines laborales.

Medidas de bajo costo y alto impacto para incorporar ciberseguridad en la PyME

Procesos

IDENTIFICAR

- Identificar los procesos y activos críticos, los indispensables para que el negocio funcione
- Identificar los proveedores esenciales para la operativa del negocio
- Identificar activos críticos: información, servidores, PCs, celulares, tablets, laptops, software, correo electrónico, impresoras, etc.

ANALIZAR

- Analizar qué hacer ante: robo, incendio, pérdida, fallo, inundación, divulgación no autorizada, etc.
- Determinar qué impacto tiene en la empresa si una de las amenazas se concreta (económico, de reputación y legal como mínimo)

DOCUMENTAR

- Respaldar la información frecuentemente y tener un juego de respaldos probado fuera de la empresa
- Definir cómo recuperar la operativa normal y en qué intervalo de tiempo.
- Definir y difundir los pasos mínimos para saber cómo actuar frente a incidentes de seguridad
- Implantar procesos de destrucción segura y borrado seguro de información sensible

Medidas de bajo costo y alto impacto para incorporar ciberseguridad en la PyME

Tecnología

DEFENSA DE PERÍMETRO

- Instalar firewalls en las conexiones a Internet y otros puntos a proteger.
- Instalar mecanismos de vigilancia como cámaras y proteger sus grabaciones.

MONITOREO

- Monitorear la actividad de los equipos para detectar comportamientos irregulares o errores de configuración.
- Utilizar software legal con soporte vigente de parches y actualizaciones.
- Actualizar frecuentemente el software y hardware, aplicar actualizaciones de seguridad a la mayor brevedad posible.
- Antivirus y antispyware con actualización automática.
- Restringir la instalación de SW para usuarios

CIFRADO Y CONTRASEÑAS

- Encriptar los medios de almacenamiento de los equipos, especialmente dispositivos móviles.
- Utilizar medios de almacenamiento removibles que admitan cifrado, como ser pendrives, y evitar la grabación de CDs y DVDs.
- Usar contraseñas de bloqueo seguras en celulares y PCs. Cambiarlas frecuentemente, utilizar letras, símbolos y números y no repetirlas o reusarlas. Si es posible, usar más de un factor de autenticación.

Recordar que la ciberseguridad es una tarea diaria y constante y un factor necesario para la PyME de hoy

¡Gracias!

¿Consultas?

@AnaKarinaLucero

@joaquinperez_b

Template: SlidesCarnival - Imogen