masempresas.cea.es
#masempresas

Fecha: Martes, Viernes 29 de Octubre 2021

Hora: **9:00h**

Duración: **1:00 h**

WEBINAR:
Cómo sobrevivir en el mundo de los ciberataques

Financiado por:

Fomento de la Cultura Emprendedora

CEA
Confederación de Empresarios de Andalucía

Junta de Andalucía
Consejería de Transformación Económica, Industria, Conocimiento y Universidades

Luis Navarro Cazorla
ciberseguridadglobal.com

Cómo sobrevivir en el mundo de los ciberataques

Ciber seguridad

Cómo sobrevivir en el mundo de los ciberataques

- **Análisis de riesgos**
  Conocer los posibles riesgos (amenazas más comunes e importantes en la actualidad) y valorar las consecuencias de los mismos sobre la empresa,

- **Gestión de riesgos**
  Disponer de conocimiento para valorar las diferentes medidas de protección y decidir la solución que más se adecue a la entidad.

- **Gobernanza**
  Información de Cumplimiento de las principales normativas, como la ley de Protección de Datos de Carácter Personal (LOPD) y el Reglamento General de Protección de Datos europeo (GDPR) o el ENS (Esquema Nacional de Seguridad), de obligado cumplimiento tanto para organismos públicos como para empresas que trabajen para los mismos.

- **Vigilancia constante**
  Observación continua de las medidas de seguridad, así como la adecuación de las mismas a la
  aparición de nuevas tecnologías.

- **Planes de contingencia**
  Determinación de las medidas a adoptar ante un incidente de seguridad.

CIBERRIESGO
MANUAL DE SUPERVIVENCIA EMPRESARIAL

(NO ES LO MISMO TRABAJAR EN LA NUBE QUE ESTAR EN ELLA…)

1. Análisis de riesgo

Ciberataques: ¿Que son y qué pretenden?

Las posibilidades de la tecnología, unida a legislación entre países, sobre todo los de fuera de la unión europea, han permitido el aumento de **acciones de hacktivismo, ciberdelincuencia, ciberterrorismo, ciberespionaje y ciberguerra**.

España es uno de los países más castigados por estas acciones delictivas.

Objetivos:

- Infraestructuras Críticas (Energía, Alimentación, Transportes)
- Administraciones públicas
- Empresas (industria, distribución, banca, seguros, sanidad, servicios).

Se detectan 14.000 nuevas formas de ataque al año, que han producido 80.000 impactos en empresas españolas, con consecuencias graves (datos 2020)

¿Qué técnicas de ataque emplean?

Las técnicas de hacking son cada vez más efectivas y rentables. Cada año se duplican los ataques y su gravedad. Ataques como el producido en el ministerio de trabajo o el CEPE son sólo dos ejemplos de esto. Destacan las botnets, ataques DDoS, ransomware y exploits que buscan, analizan y explotan las vulnerabilidades. Además se extienden los ataques a través del DNS, y se multiplican ataques a dispositivos móviles y, tras la pandemia han aumentado los ataques de ingenieria social.

Estas herramientas son producidas y vendidas en Internet (al igual que los datos obtenidos), creando el denominado “Crime-as-a-service”, donde cualquiera puede ocasionar graves pérdidas mediante el uso de armas tecnológicas.

El código dañino (Malware) alcanza mas de 1.000 millones de muestras. Fundamentalmente los malware más extendidos en la actualidad son Troyanos y Spyware.

El malware en smartphones y tablets aumenta exponencialmente.

Incidentes – Métodos de ataque

Existen una multud de métodos de ataque, tanto tecnológicos como no tecnológicos, que atentan contra la confidencialidad, integridad o disponibilidad de la información.

Los métodos de ataque van aumentando tanto por el incremento de la superficie de ataque como por la posibilidad de contar con medios de ataque más potentes y sofiscados. Están en constante evolución, afectan a uno o varios tipos a la vez y suelen usarse en combinación en el caso de objevos fuertemente protegidos.

Principales ataques

- **DDoS, robo de datos y ransomware**.
- Chantaje con ingresos empleados en la **financiación de terrorismo, tráfico de personas, armas y/o drogas**.
- **Web defacement** y otros realizados por personas cercanas a la empresa.
- En empresas, ataques de robo de datos con fines de **ciberespionaje**.

Y ante la amenaza...

El escenario no es el más idóneo

La falta de valoración de activos y definición de procesos críticos de negocio dificulta la implantación de medidas técnicas y organizativas con éxito. Provoca inversiones vagamente justificadas y poco efectivas.

Los departamentos de Asesoría Jurídica de las empresas son expertos en normativa laboral, mercantil, fiscal, etc, pero rara vez son expertos en Derecho Tecnológico. Los Departamentos de TI tampoco manejan esta materia. Los incumplimientos y sanciones en protección de datos y otras normativas son cada vez más habituales.

La escasa formación y concienciación de los recursos humanos favorece la ingeniería social, deslealtad de empleados, robo de información para entregarlos a la competencia, etc.

2. Gestión de riesgos

Impactos de un ciberataque

Sobre la IMAGEN

- Pérdida de prestigio de la marca
- Pérdida de confianza de su entorno

Sobre el NEGOCIO

- Dificultades para ofrecer el servicio a clientes en condiciones normales
- Pérdida de datos e información (de clientes, financieros, correos...)
- Posibles sanciones

Impactos de un ciberataque

Sobre los ACTIVOS

- Pérdida de confianza de proveedores / financiadores
- Posibles pagos a ciberdelincuentes

Sobre el CUMPLIMIENTO

- Sanciones derivadas por incumplimiento de normativas de privacidad
- Incumplimiento de contratos con clientes y/o proveedores
- Posibles pleitos por daños a terceros

Diferencia entre
Seguridad Informática y Seguridad de la Información

- La **seguridad de la información** es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

- La **seguridad informática** es el área de la informática que se enfoca en la protección de la infraestructura computacional y la información contenida o circulante.

El cumplimiento normativo no es garantía de tranquilidad, un responsable de ciberseguridad (diferente de un **Responsable de cumplimiemto) adopta medidas de prevención, actuación y monitorización.**

Los principales responsables de la ciberseguridad empresarial

La Ciberseguridad empresarial depende de diversas disciplinas y de profesionales especializados en los diferentes ámbitos de actuación en materia de seguridad cibernética.

Las más básicas son:

- **DPO:** tiene un perfil jurídico y de cumplimiento normativo y, según la nueva normativa europea de protección de datos, esto se exige a la administración y en algunas empresas privadas.
- **CSO:** es el responsable de la seguridad interna de la empresa. En sus manos se encuentra el establecimiento de los planes de continuidad, tener una visión completa del negocio, es necesario que ésta tenga una visión completa del negocio, conocer la normativa, conocer los posibles riesgos en Ciberseguridad, etc.
- **CISO:** la persona encargada de alinear la estrategia de ciberseguridad con los objetivos planeados por la organización. Se encarga de establecer las políticas de seguridad de la entidad en función de todas las actividades que realiza dicha organización y establecer las medidas y controles necesarios.

+ Información aquí

Los principales responsables de la ciberseguridad empresarial

Básicamente, lo normal sería contar con:

- **DPO** (personal interno responsable).
- **CSO** (responsable interno o externo del servicio técnico de sistemas, con conocimientos de ciberseguridad).
- y **CISO** (responsable interno o externo, con la gestión global de la empresa en cuanto a ciberseguridad, propuestas de mejora, notificación de incidentes según normativa, recopilación de pruebas judiciales (informática forense).

Los principales responsables de la ciberseguridad empresarial

Otros actores en la ciberseguridad:

- **ARQUITECTO DE SEGURIDAD** - Responsable del diseño de la arquitectura de ciberseguridad, su objetivo es asegurar todos los desarrollos que se lleven a cabo en el entorno tecnológico y en el cumplimiento legal en el uso de las tecnologías.
- **INFORMÁTICO FORENSE** - El encargado de hacer análisis detallados Es postmortem de sistemas y redes tras un incidente de seguridad o Ciberataque.
- **HACKER ÉTICO** - Se encuentra al día de las técnicas que utilizan los ciberdelicuentes, su labor se basa en poner a prueba los sistemas de seguridad de la organización para analizar los peligros y así ponerles remedio.
- **ANALISTAS DE SEGURIDAD** - Se encargará de detectar cualquier posible vulnerabilidad técnica en los sistemas informáticos y redes de la compañía.

3. Cumplimiento normativo

Cumplimiento normativo

- Herramientas para la ciberprotección -

Responde a la obligación en cumplimiento legal y normativo de cada actividad comercial y siempre según su nivel de riesgo.

- Normas Legales (RGPD, ENS...).
- Estándares al respecto (ISO 27001 / 20000 / 22301).

4. Vigilancia Constante (monitorizaciones)

Control y monitorización de procesos

- Herramientas para la ciberprotección -

Permite dotar al CEO de un “cuadro de mando” de la gestión de su seguridad.

- Identificación y valoración de Activos.
- Análisis de Riesgos.
- tiempo de respuesta ante incidentes.
- Roles y Responsabilidades.
- Medidas aplicadas y sus Resultados.

5. Planes de contingencia

Seguridad informática

- Herramientas para la ciberprotección -

- Proteger las vulnerabilidades propias de los sistemas informáticos:
- Planes de contingencia y continuidad.
- Tiempos de respuesta.
- Normativa de accesos y roles (plan de claves y logs de acceso).
- Sistemas antimalware.
- Copias de seguridad.
- Criptografía.

Luis Navarro Cazorla
ciberseguridadglobal.com

Preguntas y conclusiones

Cómo sobrevivir en el mundo de los ciberataques

Ciber seguridad

Información y Consultas en
masempresas.cea.es

/CEA.es @CEA.es_ /CEA.es

CEA Empresas

Gracias

Financiado por:

CEA
Confederación de Empresarios de Andalucía

Junta de Andalucía
Consejería de Transformación Económica, Industria, Conocimiento y Universidades