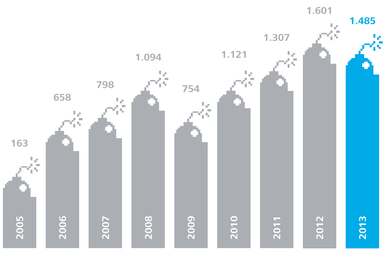
Deloitte.

Tú también puedes sufrir un ciberataque ¿Sabes cómo prevenirlo?

Número de cibereventos* publicados (2005-2013)



FUENTE: FORRESTER RESEARCH INC.

***¿Qué es un ciberevento?**
Cualquier acción maliciosa que atenta contra la disponibilidad de activos, la confidencialidad de información y la integridad de datos de una organización.

El número de cibereventos publicados en los últimos ocho años sigue creciendo, arrastrando con ello un incremento de los datos sustraídos y del número de archivos comprometidos. Esta realidad supone un riesgo para las empresas, incurriendo en altas pérdidas económicas e importantes daños de reputación.

Amenazas más comunes

Ataques a plataformas propias (web, apps, móviles...):
- Hacking
- DDoS
- Vulnerabilidad en hardware y software

Ataques a clientes (fuera de perímetro):
- Credenciales robadas
- Malware
- Phising

Ataques a activos intangibles:
- Reputación de directivos
- Reputación de marca

Ataques a activos físicos o infra-estructuras críticas:
- VoIP / Videoconferencia
- Sistema de videovigilancia
- Sucursal, tienda o cajero
- Empleado o gestor

Fraude:
- Abusos en redes sociales
- Fraude de tarjetas o cadenas de suministros
- Fraude de empleados o de terceras partes

Fuga de información confidencial:
- Pérdidas o robos de dispositivos
- Filtrado de información
- Robo de información

10 Decálogo de buenas prácticas para el ciberespacio

El factor humano es el eslabón más vulnerable de la cadena para iniciar un ciberataque. La prevención de ataques comienza con un decálogo de buenas prácticas para el ciberespacio, realizadas por el propio individuo e incorporadas a su rutina.

1. **Utilización de passwords seguras.** Una clave segura es aquella que no es de diccionario, no es pronunciable en castellano, mezcla letras, dígitos y signos de puntuación y tiene al menos 8 caracteres de longitud.
2. **Mantener actualizados todos los aplicativos de los dispositivos, incluido el antivirus.** Regularmente se debe de hacer un chequeo de todo el equipo con el antivirus.
3. **No entrar en el sistema con privilegios de administrador.** Para una navegación más segura por Internet evita conectarte desde un usuario con privilegios de administración.
4. **No dejar sesiones abiertas.** Se deben utilizar siempre los botones "logout", "salir", "cerrar sesión" o "desconectar" al abandonar un servicio web.
5. **No pinchar nunca sobre enlaces, sino teclear el enlace en el navegador.** Tampoco en enlaces que se reciban vía mensajería instantánea como chats o whatsapp.
6. **Utiliza https para una navegación segura.** Forzar a la navegación https://
7. **Desconfiar al conectar un USB ajeno.** Nunca conectar dispositivos ajenos a nuestros equipos, usbs, MP3, dispositivos móviles, discos duros externos, etc.
8. **No ignorar avisos del navegador sobre certificados de seguridad.** Los certificados de dominio son la única manera de reconocer que el sitio al que se está accediendo es legítimo.
9. **Utilizar tarjetas bancarias específicas para la compra online.** Para la compra online utiliza tarjetas que estén asociadas a cuentas bancarias dedicadas exclusivamente a compras online y controla regularmente su saldo y movimientos.
10. **La descarga no controlada o certificada de aplicaciones supone un alto riesgo para cualquier sistema o dispositivo.** Las aplicaciones descargadas en dispositivos móviles o PCs deben estar debidamente acreditadas y certificadas como legítimas y libres de malware.

Más información en:
www.deloitte.es

CyberSOC *Academy*