Microsoft Security

Consciente y seguro:

Prácticas recomendadas para salvaguardar tu empresa

Los seres humanos, y no la tecnología, representan la primera y la última línea de defensa de una organización en el cambiante panorama actual de las amenazas.

Hay que compartir la responsabilidad de la ciberseguridad. Todos tienen un papel importante que desempeñar, tanto los miembros del equipo como los profesionales de la seguridad. Juntos podemos ser ciberinteligentes y poner de nuestra parte siguiendo las prácticas recomendadas para comportarnos de forma segura online.

Aplicar prácticas de ciberseguridad inteligentes

Con la siguiente infografía sobre ciberseguridad, ayuda a todos los miembros de tu organización a comprender lo que pueden hacer para mantener su seguridad online y la de sus compañeros.

- Dispositivos — Ver la infografía >
- Estafas — Ver la infografía >
- Phishing — Ver la infografía >
- Contraseñas — Ver la infografía >

Amenazas dirigidas a los empleados

Dado que las amenazas dirigidas a los empleados tienen como objetivo a las personas, los atacantes usan tácticas de ingeniería social para engañar a los usuarios y conseguir que faciliten credenciales de acceso o revelen información confidencial.
A continuación se enumeran algunas de las tácticas más habituales.

Phishing

Los estafadores envían correos electrónicos a tus empleados simulando ser un compañero, un amigo o una persona o empresa conocida que contiene un enlace o archivo adjunto.

Spear phishing

El spear phishing, una forma más avanzada de phishing, se dirige a personas concretas (las que tienen más probabilidades de disponer de información valiosa o de acceso) en vez de a objetivos aleatorios.

Inyección de contenido

Este tipo de ataque inyecta enlaces, formularios o ventanas emergentes maliciosos que dirigen a los usuarios a un sitio web secundario en el que se les pide información confidencial, en un sitio web conocido (como un portal de banca online).

Manipulación de enlaces

Enlaces maliciosos cuyo origen parece de confianza y que llevan a los usuarios a sitios web falsos, en los que se les pide que introduzcan información de la cuenta.

Man-in-the-middle

Cuando los ciberdelincuentes engañan a dos personas para que se envíen información. El estafador puede enviar solicitudes falsas o alterar los datos que envía y recibe cada parte.

Malware

El uso normal de ordenadores, tabletas, teléfonos y otros dispositivos de puntos de conexión se ve dañado o perturbado por el malware, que incluye aplicaciones o códigos maliciosos.

Las cinco dimensiones de la ciberseguridad básica

Cómo proteger tu organización del 99 % de los ataques:

1. Habilitar la autenticación multifactor (MFA)
2. Aplicar los principios de Confianza cero
3. Usar antimalware moderno
4. Mantener los sistemas actualizados
5. Protección de datos

1 Habilitar la autenticación multifactor (MFA)

Puedes evitar el 99,9 % de los ataques a tus cuentas con la función MFA activada.[1]

Prácticas recomendadas de MFA

Es muy fácil
Selecciona para tus empleados una opción de MFA con la menor complejidad posible (como usar biometría en los dispositivos o factores compatibles con FIDO2, por ejemplo, las claves de seguridad Feitan o Yubico).

Sé prudente
Si una autenticación adicional puede ayudar a proteger datos confidenciales y sistemas críticos, elige la MFA en lugar de aplicar la autenticación en cada interacción.

Evita el trabajo del usuario final
Para evitar que los usuarios tengan que iniciar sesión varias veces para acceder a archivos compartidos o calendarios no críticos de la red corporativa cuando sus dispositivos tengan las últimas actualizaciones de software, usa políticas de acceso condicional, autenticación de paso a través e inicio de sesión único (SSO).

2 Aplicar los principios de Confianza cero

Confianza cero es la piedra angular de cualquier plan de resiliencia que desee limitar el impacto en una organización.

Principios de Confianza cero

Dar por hecho que se producirá un ataque
Asume que los atacantes pueden atacar y atacarán con éxito cualquier cosa (identidad, red, dispositivo, aplicación, infraestructura, etc.) y planifica en consecuencia. Esto significa supervisar constantemente el entorno para un posible ataque.

Verificar explícitamente
Asegúrate de que los usuarios y los dispositivos estén en buen estado antes de permitir el acceso a los recursos. Valida explícitamente que todas las decisiones de confianza y seguridad usen la información y telemetría pertinentes disponibles para proteger los activos contra el control de los atacantes.

Usar el acceso con privilegios mínimos
Usa el acceso puntual y suficiente (JIT/JEA) y las políticas basadas en el riesgo, como el control de acceso adaptativo, para limitar el acceso a un activo potencialmente comprometido. Solo debes permitir los privilegios necesarios para acceder a un recurso y nada más.

3 Usar antimalware moderno

Usar antimalware de detección y respuesta extendidas. Implementar software para detectar y bloquear ataques automáticamente y proporcionar conocimientos a las operaciones de seguridad.

4 Mantente actualizado

Los sistemas sin parches y desactualizados son uno de los principales motivos por los que muchas organizaciones son víctimas de un ataque. Asegúrate de que todos los sistemas se mantengan actualizados, incluido el firmware, el sistema operativo y las aplicaciones.

Tres prácticas recomendadas

Aplicar parches
Asegúrate de que los dispositivos sean robustos aplicando rápidamente parches y cambiando las contraseñas predeterminadas y los puertos SSH predeterminados.

Reducir
Elimina las conexiones a internet y los puertos abiertos innecesarios y restringe el acceso remoto mediante el bloqueo de puertos, la denegación del acceso remoto y el uso de servicios de VPN.

Segmentar
Segmenta las redes para limitar la capacidad de un atacante de moverse lateralmente después de la intrusión inicial. Los dispositivos del IoT y las redes de TO deben aislarse de las redes corporativas de TI mediante firewalls.

5 Protección de datos

Conocer los datos importantes, dónde se encuentran y si se han implementado los sistemas adecuados es crucial para implementar la protección adecuada.

Consulta La ciberhigiene básica previene el 99 % de los ataques para obtener más información sobre las prácticas de ciberhigiene detalladas anteriormente.

Diez consejos esenciales para proteger tu red

1. Proporciona a tus empleados formación sobre el correo electrónico y la navegación seguros.
2. Ofrece formación sobre la simulación de ataques en Microsoft Defender para Office 365.
3. Prescinde de las contraseñas y usa MFA.
4. Asegúrate de que todos los dispositivos de la empresa utilicen la última versión de Windows y del navegador de Internet.
5. Aplica protocolos corporativos de almacenamiento de archivos. Almacena y cifra los datos de la empresa de forma segura en el cloud.
6. Forma a los empleados sobre las conexiones seguras. Instala el complemento HTTPS Everywhere para tu navegador.
7. Forma a los empleados para que verifiquen la identidad de los sitios web comprobando sus certificados.
8. Para garantizar entornos seguros, explora las prácticas recomendadas de automatización y las estrategias de gestión de los datos.
9. Habilita los bloqueadores de elementos emergentes de forma predeterminada.
10. Utiliza soluciones antivirus basadas en el cloud como Microsoft Windows Defender.

1. https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

Explorar más prácticas recomendadas de ciberseguridad y oportunidades de formación en https://aka.ms/cybersecurity-awareness.

Microsoft Security