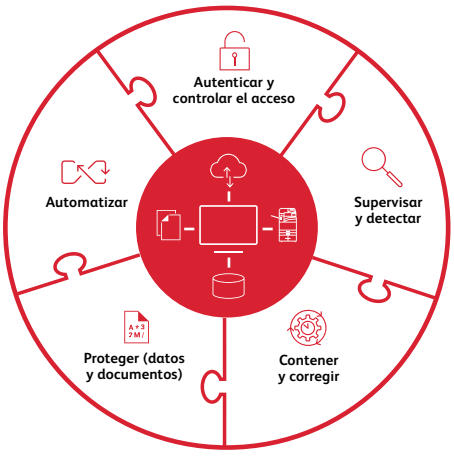
Confianza cero

La ciberdelincuencia ha alcanzado niveles sin precedentes a nivel global y se espera que siga creciendo. Las organizaciones necesitan estrategias nuevas y buenas prácticas para defenderse contra estas amenazas.

La fuerza de trabajo distribuida de hoy en día necesita acceder a su infraestructura de TI en cualquier momento y desde cualquier lugar. Cada vez más iniciativas de transformación digital están facilitando el acceso a los datos empresariales. Ahora hay una gran cantidad de dispositivos IoT conectados a sistemas empresariales críticos, que constituyen la columna vertebral de cualquier negocio. Estas tendencias están poniendo a los profesionales de seguridad bajo una presión cada vez mayor para habilitar el lugar de trabajo moderno y, al mismo tiempo, reducir la superficie de ataque a la seguridad de la empresa.

La confianza cero ha surgido como un potente método para proporcionar acceso seguro a los usuarios y dispositivos autorizados, al tiempo que mejora la estrategia de seguridad empresarial.

Con la seguridad integral como objetivo clave de Xerox, hemos dotado a nuestros clientes de productos y servicios que respaldan las iniciativas de Confianza cero. Conceptos como "nunca confíes, siempre verifica", "acceso con mínimos privilegios", "detección y corrección proactiva de amenazas", "cifrado" y "certificaciones de seguridad" no son nuevos. Sin embargo, cuando se utilizan en una estrategia de seguridad cohesionada, representan funciones críticas de un programa de seguridad de Confianza cero satisfactorio.



Implementación de Confianza cero

Apoyamos sus iniciativas de Confianza cero con las siguientes buenas prácticas y recomendaciones:

AUTENTICAR Y CONTROLAR EL ACCESO

Comience con la política de "confianza implícita" y asegúrese de que se comprueba el acceso de todos los usuarios.

Las impresoras Xerox® se envían desde fábrica con contraseñas exclusivas y seguras para la cuenta de administrador. Los controles de acceso basados en roles pueden implementarse con nombres de usuario locales, acceso mediante código PIN, a través de tarjetas y autenticación segura con CAC/PIV. Es posible imponer un acceso de privilegios mínimo y una validación continua con temporizadores de inactividad/desconexión. La autenticación multifactor es posible a través de proveedores de identidades en la nube como Ping Identity, Okta, Microsoft Azure Identity Services y las soluciones para el lugar de trabajo Xerox® Workplace Cloud/Xerox® Workplace Suite.

Las soluciones de gestión de la impresión Xerox® Workplace Cloud y Xerox® Workplace Suite amplían las capacidades de las impresoras Xerox® en todo un parque de dispositivos para proporcionar un enfoque coherente. Imponen una postura de seguridad de "nunca confiar" exigiendo a los usuarios que desbloqueen las impresoras con tarjetas/etiquetas, dispositivos móviles o códigos PIN antes de acceder a los servicios disponibles de las impresoras.

Servicios de impresión gestionados (MPS) de Xerox® implementa la autenticación obligatoria en cada nueva conexión a nivel de usuario y de sistema. Establece un acceso definido en base a las funciones del usuario y gestiona las contraseñas con los métodos aprobados por NIST 800-171R2. La gestión de CA/certificados garantiza que las impresoras autorizadas se comuniquen de forma segura a través de la red.

SUPERVISAR Y DETECTAR

Controle y detecte continuamente las amenazas (potenciales) a la seguridad.

Las impresoras Xerox® están equipadas con firmware firmado digitalmente y cifrado, y con la verificación del firmware, están diseñadas para protegerse de los intentos de manipulación del software del sistema. Las Trellix*[1] Listado blanco/Permitir listado supervisan el malware en tiempo real, rechazando y notificando a los usuarios cualquier actividad maliciosa. Trusted Boot[4] garantiza la integridad del proceso de inicio del sistema.

La generación de datos de registro Syslog/Audit y la integración con herramientas SIEM[2] como LogRhythm, Splunk y Trellix* Security Manager proporcionan información útil para detectar y mitigar las amenazas a la seguridad. Con la ayuda de Cisco Identity Services Engine (ISE), podemos detectar e impedir que impresoras no autorizadas se conecten a su red.

Xerox® Workplace Cloud y Xerox® Workplace Suite se integran con su sistema de gestión de identificación para garantizar un acceso y un funcionamiento de la autenticación sin problemas. Así se evitan problemas de sincronización entre el mecanismo de control de acceso y el proveedor de ID. A nivel local/del dispositivo, utilizamos herramientas como reCAPTCHA para supervisar y bloquear los intentos de entrada por la fuerza detectados.

Los Servicios de impresión gestionados de Xerox® ofrecen una cadencia de supervisión de la seguridad definida por el cliente. Implementamos la gestión de dispositivos en todo el parque con el Servicio de auditoría de seguridad de las impresoras Xerox®. Se utiliza para gestionar la configuración de todo el parque de forma intuitiva mediante políticas de seguridad e impresión en remoto. También se utiliza como base para la elaboración de informes de datos interactivos en tiempo real. Las revisiones de seguridad y las actualizaciones de firmware se aplican de acuerdo con la política de seguridad del cliente.

xerox™

Confianza cero

CONTENER Y RESOLVER

En caso de un posible peligro, contener la amenaza y proporcionar una solución rápida para eliminarla.

En Xerox, hemos diseñado nuestras impresoras con un enfoque de seguridad desde el principio que evita que las amenazas las infecten. Las capas de funciones de seguridad contienen aún más posibles brechas de seguridad. Por ejemplo, la función de impresora Vigilancia de configuración[3] permite a los administradores del sistema implementar hasta 75 opciones de seguridad y corregirlas (restablecerlas) de forma proactiva en caso de que se cambien.

A nivel de parque, los Servicios de auditoría de seguridad de las impresoras Xerox® mantienen el cumplimiento de las políticas y corrigen de forma proactiva todos los dispositivos que no cumplan. Realizamos revisiones periódicas de las políticas de configuración (para garantizar que están actualizadas con los requisitos de seguridad), asesoramos al cliente y proporcionamos recomendaciones de seguridad continuas.

PROTEGER (DATOS Y DOCUMENTOS)

Utilice técnicas de cifrado de datos y soluciones de software para proteger los datos y documentos de su divulgación intencionada y no intencionada.

Las unidades de almacenamiento de nuestras impresoras están protegidas con cifrado de 256 bits. Los datos almacenados que ya no son necesarios pueden borrarse mediante algoritmos de limpieza y borrado de datos aprobados por el Instituto Nacional de Normas y Tecnología (NIST) y el Departamento de Defensa de los EE. UU. La salida de impresión está protegida mediante el uso de un PIN o un sistema de liberación mediante tarjeta. Además, evitamos que la información escaneada llegue a quienes no deberían recibirla, utilizando formatos de archivo firmados digitalmente, cifrados y protegidos con clave.

Nuestras impresoras[4] le permiten bloquear los campos de correo electrónico "para/cc/cco", limitando los destinos de escaneado solo a los dominios designados, como los internos. Con la función de Seguridad de reproducción de imágenes, las impresoras Xerox® AltaLink® utilizan tecnología IR (infrarrojos) para marcar y detectar documentos confidenciales. Así se evita su duplicación no deseada y se crean alertas y registros de auditoría para rastrear los intentos de duplicación.

Los servicios de red no utilizados pueden desactivarse para reducir la superficie de ataque de la red. Se puede implementar el Filtrado de IP para restringir el acceso a la red solo a los clientes autorizados para escanear, imprimir y administrar los equipos dispositivos. Protocolos seguros como IPsec, HTTPS, LDAPS y SFTP protegen los datos en tránsito. El modo FIPS puede activarse para garantizar que solo los protocolos más seguros puedan interactuar con el dispositivo.

La solución Xerox® Workplace Cloud cifra el contenido en tránsito y en reposo. El contenido almacenado en la nube de Xerox puede cifrarse mediante la propia clave de cifrado del cliente. Al utilizar su propia gestión de cifrado, los clientes obtienen todas las ventajas de pasarse a una gestión de impresión basada en la nube y mantienen el control sobre quién puede ver el contenido de sus datos. La función de Seguridad del contenido de las soluciones Xerox® Workplace Cloud y Workplace Suite permite detectar contenido confidencial predefinido y generar alertas e informes basándose en cómo se usan los datos.

Los Servicios de auditoría de seguridad de las impresoras Xerox® garantizan que los datos y las funciones de protección de documentos están activados en el parque, corrigen infracciones de políticas e informan del cumplimiento.

AUTOMATIZAR

Racionalice la política de seguridad para obtener los mejores resultados.

La automatización da lugar a la simplicidad y permite a los equipos de seguridad centrarse en cuestiones importantes. La función del Orquestador del parque de equipos Xerox® automatiza la configuración de los dispositivos y aplica las actualizaciones de firmware a una red de impresoras. Así se garantiza el cumplimiento al tiempo que se reduce la carga de trabajo del personal de TI. Con la integración de Cisco ISE y Trellix* ePolicy Orchestrator, cualquier impresora puede ponerse en cuarentena automáticamente al detectar una amenaza. De este modo se evitan daños en la impresora y se protege la red y otros puntos finales.

Los Servicios de auditoría de seguridad de las impresoras Xerox® utilizan un mecanismo centralizado de políticas y la agrupación de dispositivos para racionalizar la gestión del parque con el mínimo esfuerzo. La aplicación y comprobación del cumplimiento está totalmente automatizada. Los paneles presentan información sobre el cumplimiento del parque, las políticas y los dispositivos en un formato gráfico fácil de leer.

El éxito de un programa de seguridad depende de una política de seguridad sencilla y ejecutable, respaldada por funciones y servicios de productos que garanticen el cumplimiento. La Confianza cero se está convirtiendo rápidamente en el modelo de seguridad preferido por empresas de todos los tamaños. Mediante la implementación de las recomendaciones de seguridad de Xerox descritas en este informe, las empresas pueden proporcionar acceso de usuario autorizado de forma segura, limitar la exposición en caso de filtraciones de datos y automatizar las respuestas a posibles amenazas de seguridad.

[1] Equipos multifunción Xerox® AltaLink®, Serie EC y Xerox® VersaLink® serie 7100.
[2] Integración directa de AltaLink® en SIEM, todos los demás dispositivos a través de los Servicios de impresión gestionados (MPS) de Xerox®.
[3] Equipos multifunción Xerox® AltaLink® series 8000 y 8100.
[4] Xerox® AltaLink® y Xerox® VersaLink®.
*Trellix anteriormente conocido como McAfee.

Para obtener más información sobre la seguridad de Xerox, visite **www.xerox.es/es-es/quienes-somos/soluciones-de-seguridad**.