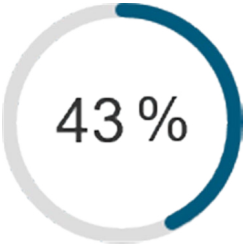
Elementos esenciales de seguridad en las pymes

A la cabeza en todo lo relacionado con la seguridad

Descubra cómo es el panorama actual de las ciberamenazas a las pymes para que su empresa pueda sobrevivir; reduzca los costes operativos y crezca de manera segura. Haga de la seguridad una prioridad para todos y proteja su negocio con Cisco.

A medida que crece su empresa, llama la atención y no toda es bienvenida. Cada vez hay más bandas criminales sofisticadas detrás de las pymes.



Un 43 %
de las pequeñas empresas objetivo de los ciberataques. [1]

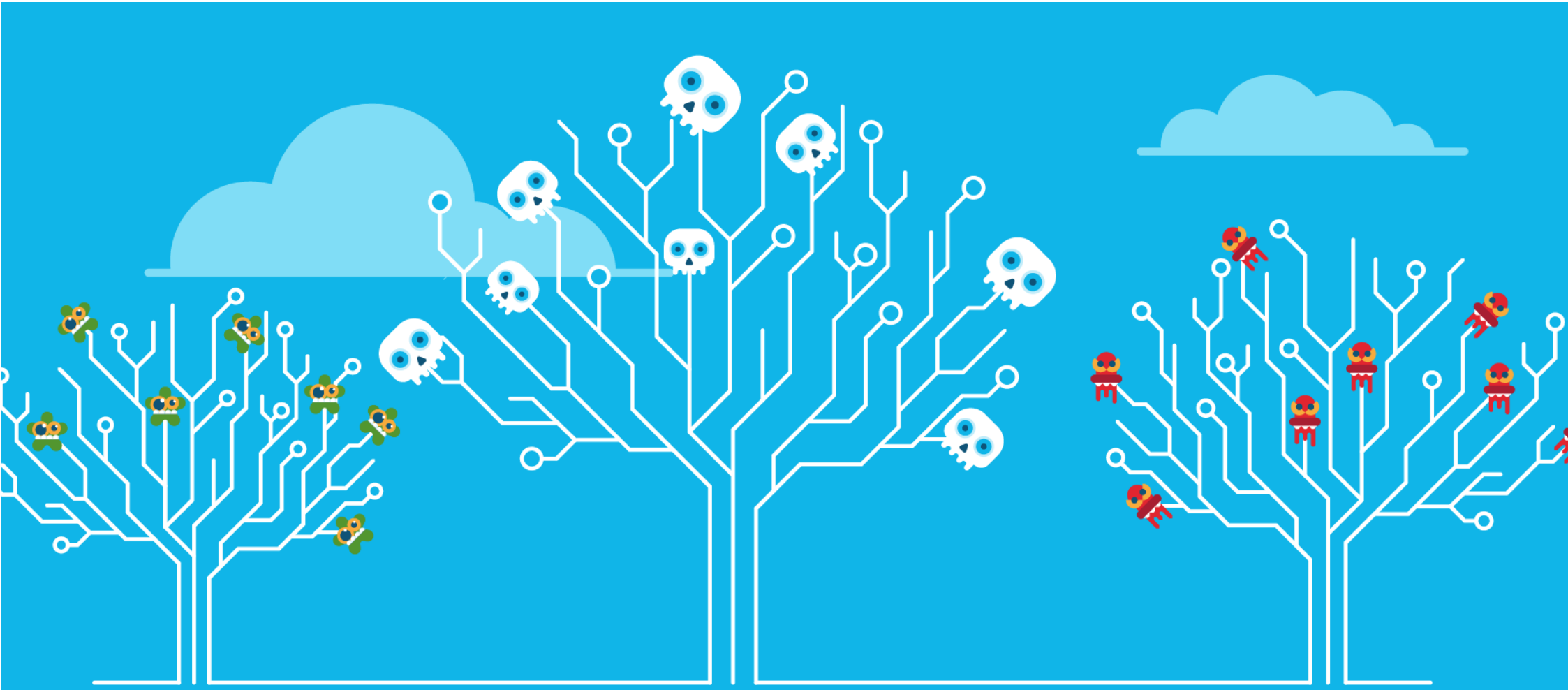
Como resultado, un 60 %
de ellos se verán obligados a cerrar. [1]

Informe anual de ciberseguridad de Cisco 2018 “Cisco ACR 2018”.

2 235 018 USD al año

El importe medio que gastan las pymes a consecuencia de un ciberataque o una brecha de datos debido a los daños o al robo de recursos de TI y a la interrupción del proceso de operaciones normal.

Es una verdad amarga que implica que la supervivencia de su empresa depende de la comprensión en seguridad cibernética.



Las amenazas se están volviendo más sofisticadas

Los hackers conocen sus debilidades y cómo explotarlas

Hoy día hay menos hackers que lo hacen “solo por diversión” o como un reto. La mayoría están motivados por el dinero, están bien organizados y pocas veces trabajan solos. Los atacantes son ágiles, mientras que las empresas no siempre pueden decir lo mismo. Especialmente cuando acaban 'conformándose' con la seguridad.

El objetivo del hacker es robar información de tarjetas de crédito, direcciones de correo electrónico, nombres de usuario y contraseñas. Cualquier cosa que pueda venderse al mejor postor. *Sus métodos de actuación* pueden incluir algunas de las siguientes técnicas.

Ransomware

Los atacantes pueden tener a las empresas como rehenes de forma virtual mediante un ransomware; una práctica implacable. El ransomware cifra sus archivos de forma remota y sin su consentimiento. Algunas formas de ransomware también se programan para que se propaguen a través de la red.

En lugar de obligar a un destinatario a abrir un correo electrónico adjunto o hacer clic en un enlace, las tendencias actuales en ransomware, como WannaCry, que se inicio en mayo de 2017, permiten que se transmita un código malicioso entre redes, sin interactuar con el usuario. “WannaCry es el primero en ser totalmente automatizado”, afirma Craig Williams, gerente sénior de ampliación de seguridad en Talos, la empresa que se encarga de las investigaciones de seguridad para Cisco.

WannaCry afecta a más de 200 000 ordenadores en todo el mundo y puede provocar una pérdida estimada en 4000 millones de USD. WannaCry se instala a través de una vulnerabilidad en el protocolo SMB de Microsoft y es particularmente eficaz en entornos antiguos de Windows, como Windows XP, Windows Server 2003 y Windows 8. Microsoft ya ha lanzado una actualización de seguridad para aplicar un parche sobre esta vulnerabilidad, pero no todos los usuarios estaban protegidos de forma automática.

Pymes como rehenes

El 52 % de las pymes que ha participado en el informe “2017 State of Cybersecurity in Small and Medium-Sized Businesses” de Ponemon Institute, han sufrido ataques de ransomware con y sin éxito en un periodo de 12 meses. Una vez que se ha llevado a cabo la infección, aparecerá un mensaje en la pantalla pidiendo que pague un rescate en bitcoins por no revelar sus datos. El rescate típico puede oscilar entre las 200 £ y las 10 000 £, pero algunas víctimas han llegado a pagar un precio mucho más alto.
Los titulares recientes informan de una nueva generación de amenazas que se han hecho virales a escala global y que se están propagando más rápido que nunca. El grupo de investigación contra amenazas Cisco Talos ha descubierto una nueva, llamada VPNFilter, que compromete a más de 500 000 routers y redes conectados a

dispositivos de almacenamiento alrededor del mundo de oficinas pequeñas u hogares. Los dispositivos de Cisco no se encuentran entre los afectados. Estas amenazas complejas permiten que el agente inspeccione el tráfico que circula por los dispositivos para robar archivos de las unidades de copia de seguridad de la red y que posiblemente acceda a las redes corporativas conectadas.

Los cibercriminales conocen a sus víctimas, indagan en lo que les gusta y no les gusta y en cómo dirigen sus empresas. Saben lo que pagarán para que no se divulguen sus datos y explotan despiadadamente cualquier debilidad que encuentren.

Comprometer los correos electrónicos empresariales (BEC)

Comprometer el correo electrónico empresarial (BEC) significa un 75 % más de rentabilidad de la que da el ransomware. A pesar de ello, no tiene tanta publicidad.

El BEC son ataques dirigidos en los que los hackers utilizan ingeniería social para engañar a personas para que les transfieran dinero. No hay ningún malware ni archivos adjuntos. A diferencia de los ataques de ransomware, no toman ningún dato de sus víctimas. Todo se basa en mentiras e instrucciones para confundir.

Normalmente, los hackers dedican tiempo a investigar a la empresa que tienen como objetivo y empiezan construyendo un perfil. Cuando tienen suficiente información, envían correos de suplantación de identidad a empleados veteranos de la empresa, a menudo del departamento de finanzas. Debe ser alguien con autoridad para transferir el dinero. Cuanto mayor sea la empresa, más dinero pueden generar. Sin embargo, están aumentando los ataques dirigidos a pequeñas y medianas empresas.

Cuanto mayor sea la empresa, más dinero pueden generar. Sin embargo, están aumentando los ataques dirigidos a pequeñas y medianas empresas.

Brecha de datos

Los datos están en el corazón de todo lo que hace su empresa: es su propiedad intelectual, su siguiente gran oportunidad, sus registros de clientes, sus ingresos. Una brecha supone mucho más que solo solucionar las interrupciones y arreglar los sistemas con daños.

El crear una condición en materia de seguridad sólida puede ayudarle a proteger su propiedad intelectual y su reputación. De media, las organizaciones tardan 191 días en detectar una brecha y 66 días en contenerla. (Fuente: Ponemon Institute). Sin embargo, la clave para limitar los daños es detectarla lo antes posible.

El promedio de tiempo de Cisco para detectar las brechas es de 3,5 horas. Si se produce una brecha, los expertos de los Servicios de respuesta a incidentes de Cisco están disponibles en cuestión de horas para ayudarle a controlar y solucionar las causas principales.

Ataques en la cadena de suministros

Los ataques en la cadena de suministros son una ciberamenaza emergente y cada vez mayor, que demuestra lo especializados que están los ciberdelincuentes. Lo que sucede es que los malos ponen en peligro los mecanismos de actualización de software de los paquetes de software (por lo demás, legítimos). Esto les permite superponerse en la distribución de un software original.

Fundamentalmente, los cibercriminales tendrán como objetivo una empresa de la cadena de suministros con prácticas de seguridad cibernética débiles, especialmente cuando se trata de compartir información. Por esta razón, las pymes suelen ser el objetivo.

Una vez que han identificado el punto débil, el atacante puede centrarse en la explotación objetivo final pretendido.

Defensa contra atacantes en todas partes

No permita que los atacantes frenen su negocio. Luche contra ellos en todos los sitios en los que intenten entrar. Nuestras soluciones le protegen desde la capa de DNS hasta el correo electrónico y los terminales. Además, están respaldados por Talos, el equipo de investigación de amenazas líder en el sector.

Qué hacer

Si ocupa un lugar en una cadena de suministros, pregunte a sus proveedores/partners cómo protegen sus cadenas de suministros. Pregúnteles sobre sus prácticas de desarrollo y sus controles de seguridad internos. ¿Cómo ejecutan parches y actualizaciones en sus sistemas internos y con qué frecuencia? ¿Cómo segmentan y protegen sus entornos de desarrollo, control de calidad y producción? ¿Cómo examinan a sus partners y proveedores?

Asegúrese de plantear todas estas preguntas sobre su organización o podría darse cuenta de que su organización es el eslabón más débil de la cadena de suministros.

Para obtener más información acerca de los ataques en la cadena de suministros: https://gblogs.cisco.com/uki/protecting-...

Demasiadas empresas tienen un “problema de acumulación”

Algunas empresas no tienen clara su estrategia de seguridad cibernética. Hacen lo posible con una solución hasta que se convierte en un impedimento.

Otras intentan considerar todas las posibilidades y acabar con un problema de acumulación. Una acumulación de varias soluciones de seguridad de punto de diferentes proveedores utilizadas a la vez. Ambas situaciones conllevan problemas.

Esta acumulación de tecnologías de seguridad incompatibles deja brechas y crea problemas de gestión e ineficiencias que desarrollan los hackers. Cada nueva solución de seguridad viene con otra interfaz de gestión. Cada nueva solución requiere recursos humanos, horas de gestión para su configuración, establecer políticas y responder a las alertas, y no está siempre claro si el resultado adicional obtenido en términos de seguridad merece todo el esfuerzo extra que hay que dedicar a gestionarla, en lugar de centrarse en problemas más importantes.

Puede que haya añadido complejidad sin aumentar mucho la efectividad global. Esta situación se ve agravada por el hecho de que la seguridad aún se ve principalmente como un “problema de TI”. Según el estudio comparativo de seguridad de Cisco, algunas organizaciones no están totalmente de acuerdo con que los responsables de las líneas de negocio se comprometan con la seguridad. La actitud suele ser: “la seguridad es un problema de TI”. Esto es un verdadero problema, ya que implica que la seguridad se “añade” en lugar de integrarse en el ecosistema de la empresa. El ahorro crea más trabajo.

Cuando se aplica correctamente, la seguridad puede facilitar los negocios. Una plataforma para el crecimiento.

La “superficie de ataque” es cada vez más grande y más complicada

Trabajamos en todas partes: desde casa, en la oficina, aeropuertos o cafeterías. Sin embargo, las soluciones de seguridad tradicionales todavía se centran en proteger a los empleados solo en la red empresarial.

Imagínese esta escena:

- Los usuarios acceden a su red desde sus propios dispositivos inteligentes, allá donde estén

- Las aplicaciones, servidores y datos de su negocio están en la nube

- Los dispositivos que ni siquiera parecen ordenadores conectados a sus redes (piense en medidores inteligentes, termostatos, impresora, cámaras...)

- Y para complicar más la trama, necesita descubrir cómo conseguir seguridad en todas partes para proteger esta compleja infraestructura

TI en la sombra

La TI en la sombra es una práctica en la que los empleados utilizan cualquier aplicación que quieren, sin tener la aprobación del departamento de TI. Puede ser cualquier cosa, desde instalar un programa de mensajería instantánea en un dispositivo corporativo, hasta descargar su propio software de uso compartido de archivos y utilizarlo para transferir datos confidenciales.

De los encuestados que participaron en el informe 2017 State of Cybersecurity in Small and Medium-Sized Businesses (SMB) de Ponemon Institute que sufrieron una brecha de datos, el 54 % indicaba que los empleados negligentes eran el origen del problema, un aumento con respecto al 48 % de los encuestados en el estudio del año anterior.

La TI en la sombra puede crear grandes vulnerabilidades de seguridad, sobre todo si desconoce el alcance que puede tener el problema. Este tipo de operación es como nadar en un océano repleto de tiburones con un bañador de carne. Sin embargo, es sorprendentemente frecuente en las empresas. Entonces, ¿por qué sucede?

Para ser justos con el personal, sucede con las mejores intenciones. Los trabajadores quieren mejorar sus niveles de productividad y utilizan las herramientas digitales más recientes. El personal no suele pensar en las implicaciones de seguridad cuando acceden a estas aplicaciones. A veces, los empleados utilizan herramientas de TI en la sombra porque estaban acostumbrados a utilizar determinados sistemas en su organización anterior. Después de todo, resulta más fácil que aprender algo nuevo.

Arrojar luz sobre la TI en la sombra

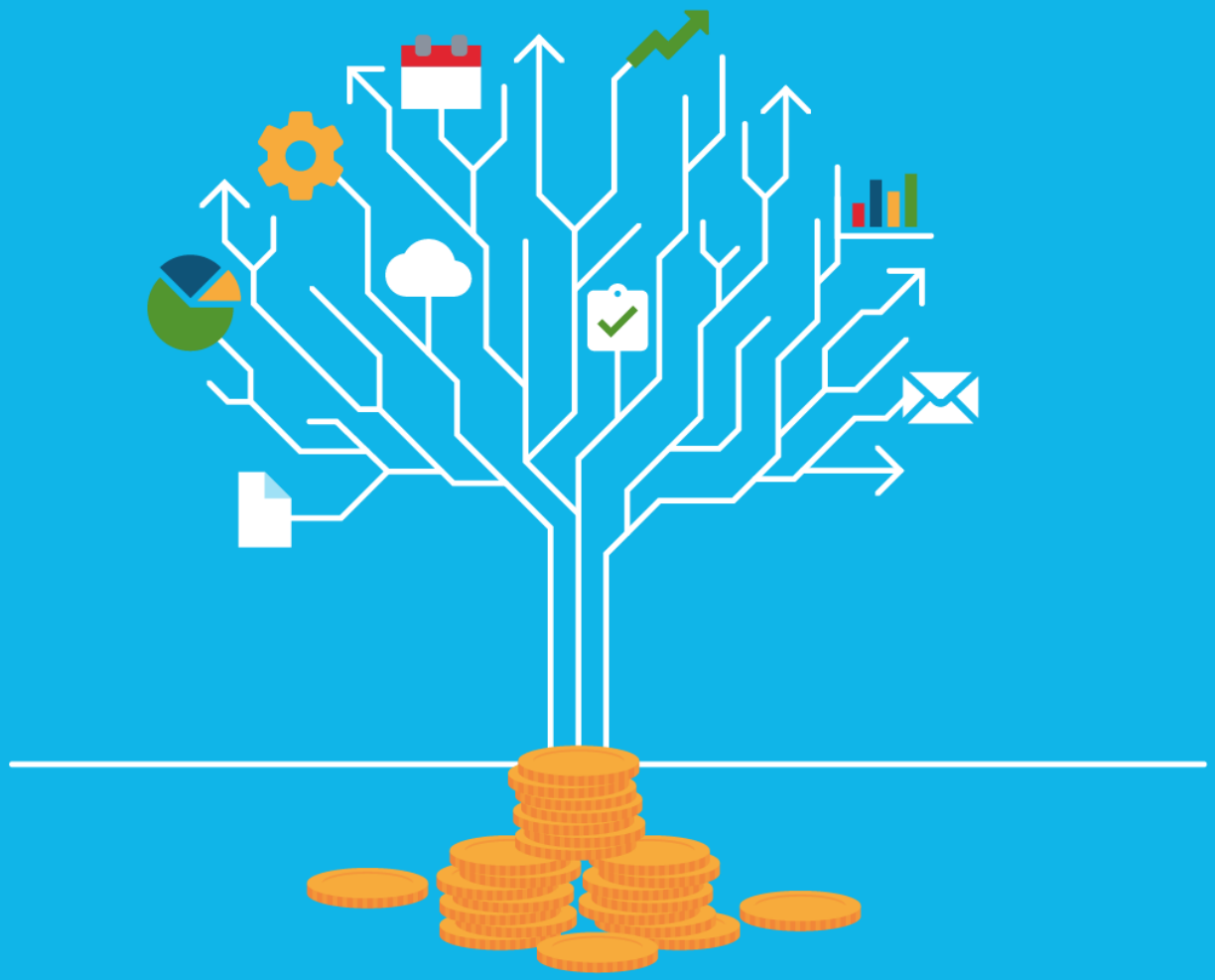
Es posible transformar la TI en una contribución positiva para su empresa:

- Si aún no lo ha hecho, configure un foro o una herramienta de “ideas de los empleados” que permita a sus empleados proponer ideas que pueden mejorar el funcionamiento de la empresa. Recompense a los que los hagan y celebre cuando una idea se convierta en realidad.
- Una seguridad efectiva no depende solo de la tecnología, también depende de establecer los procesos adecuados. Haga que la conciencia de la seguridad sea una parte fundamental de su programa de formación para que la gente entienda las consecuencias de utilizar dispositivos y programas peligrosos.
- Conocer lo que ocurre en su red es una gran prioridad en la seguridad de TI. Por desgracia, la mayoría de las empresas no saben cuándo se ha producido una brecha, cómo ocurrió o el daño que puede ocasionar. Evítelo.

Política de contraseña

Las contraseñas robustas siguen desempeñando un papel fundamental en la ciberseguridad para pymes. Sin embargo, el 59 % de los encuestados en el informe Ponemon actual, el mismo porcentaje que en el informe anterior, afirma que no tienen visibilidad en las prácticas de las contraseñas de los empleados, incluido el uso de contraseñas únicas o fuertes.

Además, los encuestados afirman que las políticas de contraseña no se aplican estrictamente. Si una empresa tiene una política de contraseñas (el 43 % de los encuestados la tiene), el 68 % afirma que no se aplica estrictamente o no están seguros del grado en el que se administra.



El crecimiento requiere seguridad

La debilidad cibernética perjudica a la innovación

Bloquear los ciberataques es sin duda una gran preocupación, pero su impacto en el crecimiento y la innovación de la empresa es el resultado más preocupante de tener una ciberseguridad débil.

En un estudio reciente realizado por Cisco, un asombroso 71 % de los ejecutivos afirmó que la preocupación por la ciberseguridad había impedido la innovación en sus empresas. Entre los encuestados, el 39 % afirmó que habían frenado iniciativas vitales debido a los problemas de ciberseguridad. Estas respuestas destacan cómo la debilidad de la ciberseguridad disminuye la capacidad de las empresas para innovar precisamente en el momento en el que necesitan hacerlo para competir.

La digitalización, la revolución y el cambio exponencial se han convertido en la nueva normalidad de un entorno empresarial altamente competitivo. Las empresas ágiles pueden establecer una clara ventaja sobre la competencia si pueden innovar, actuar con rapidez y recompensar la experimentación.

Un impacto de una brecha va más allá del balance final

Un fallo a la hora de proteger su red puede tener consecuencias de largo recorrido, por ejemplo: tiempo de inactividad, daños y sustitución del equipo, respuesta a incidentes, investigaciones forenses, inspecciones internas y comunicaciones.

Una pérdida de la confianza del cliente puede dañar de forma permanente una fuente de ingresos que antes era sólida. Perder los datos de sus clientes puede suponer acciones legales, multas, aumento de la regulación y gastos de reparación. Sin embargo, los daños no se detienen aquí. Por ejemplo, si un vendedor sufre una brecha de datos, los clientes dudarán si volver a compartir su información personal.

Su empresa puede obtener una ventaja decisiva aprovechando:

- Las tecnologías establecidas como la web, el móvil, la nube, la gestión de recursos empresariales y la gestión de la relación con los clientes

- Las tecnologías de desarrollo rápido como la inteligencia artificial y el análisis de datos

Estas tecnologías ayudan a las empresas a conectar mejor con sus clientes, acceder a nuevos mercados y mejorar la productividad de los trabajadores, a la vez que aumentan los ingresos y reducen los costes. Las preocupaciones sobre la ciberseguridad pueden dificultar la búsqueda de modelos empresariales digitales e innovaciones.

Está condenado tanto si lo hace como si no

Muchos empresarios realizan una mala elección. El riesgo de hacerlo de forma errónea o el riesgo de quedarse atrás. Sienten que deben continuar

avanzando o arriesgarse a verse sobrepasados por la revolución digital y otros competidores más ágiles. En nuestra encuesta, el 73 % de los encuestados admitieron que suelen adoptar nuevas tecnologías y procesos empresariales a pesar de los riesgos que implica la ciberseguridad.

La ciberseguridad por debajo del nivel esperado deja a las empresas en la peor posición competitiva posible: no innovan lo suficientemente rápido como para competir ni tampoco cuentan con medidas suficientemente seguras como para evitar los ciberataques, a pesar de retrasar innovaciones digitales.

¿Cómo afectaría a su empresa una brecha de seguridad o un ataque de ransomware?

¿Cuál es el posible impacto financiero de una interrupción de la red debido a una brecha de seguridad o la pérdida de acceso a datos y sistemas debido a un ataque de ransomware?

- ¿Podría interrumpir su cadena de suministro una brecha de seguridad o un ataque de ransomware?
- ¿Qué pasaría si un ataque causa la caída de su sitio web?
- ¿Su empresa depende de las características de comercio electrónico de su sitio web?
- ¿Cuánto tiempo podría estar el sitio caído antes de que su empresa perdiese dinero?
- ¿Su empresa está asegurada frente a ciberataques o frente al uso indebido de los datos de sus clientes? ¿Este seguro es adecuado?
- ¿Su empresa tiene capacidades de copia de seguridad y recuperación para restaurar la información, si es necesario, después de una brecha de seguridad o una pérdida de datos debida a un ataque de ransomware?

Valor digital en juego

El valor digital en juego es una manera de ubicar un valor con seguridad. Se basa en fuentes de valor totalmente nuevas que surgen de las inversiones en innovaciones e iniciativas digitales, y el valor cambia entre empresas en función de su capacidad para aprovechar las funciones digitales.

Una parte del valor digital en juego viene de la perspectiva defensiva de la ciberseguridad, como por ejemplo:

- Protección de la propiedad intelectual
- Reducción de datos comprometidos (tanto internos como información de cliente), aumento del tiempo de actividad empresarial y reducción del tiempo de inactividad de la red
- Protección de activos financieros
- Protección de información política, nacional y gubernamental confidencial
- Preservación de la reputación de la empresa

Obtenga la perspectiva completa. Lea la Guía más reciente sobre ciberseguridad para impulsar la rentabilidad de Cisco.

Una plataforma segura para el crecimiento

La arquitectura de seguridad integrada de Cisco ayuda a las empresas a mejorar la eficacia en materia de seguridad, al minimizar el tiempo necesario para detectar amenazas y resolver incidentes, impulsar el ahorro (tanto en el desembolso de capital como en los gastos operativos) y mejorar la productividad del personal de TI.

Integrar a todo el mundo con seguridad cibernética

Haga de la seguridad una prioridad para todos

A veces es necesario un gran golpe para que todo el mundo se sume a las iniciativas de seguridad cibernética.

El 60 % de las pymes que sufren una brecha de seguridad cibernética se ven forzadas a cerrar. Lo que significa, especialmente para usted, que es mejor prevenir que curar.

Presentar los factores de riesgo específicos para su empresa

Ayude a su junta directiva a comprender las amenazas de seguridad que puedan afectar a su organización en particular. No pierda demasiado tiempo presentando estadísticas y tendencias genéricas. En su lugar, ayúdeles a ver la conexión entre esas tendencias de seguridad y los retos que son muy específicos de su empresa y su sector. Cuanto más contexto pueda proporcionar, más relevante será para ellos.

Por ejemplo, puede hablarles de la mayor fuente de ingresos de su empresa y darles ejemplos de cómo las amenazas de seguridad como el ransomware podrían suponer una amenaza. Si su empresa conserva datos confidenciales, como registros financieros, podría mostrar ejemplos de las implicaciones legales y las multas en las que podría incurrir su organización si dichos datos se hicieran públicos.

Muéstreles cómo funciona un ataque, lo fácil que puede ser comprometer la seguridad. Ofrézcales ejemplos reales de los problemas a los que ya se enfrentan, así como de los riesgos y los efectos a largo plazo que podrían tener esos problemas.

Cuantificar todo

A los ejecutivos les gustan sus métricas y sus números. Por lo tanto, es importante que alinee sus prioridades de seguridad con los objetivos y los plazos de su empresa. Conozca sus prioridades empresariales y de TI y muestre cómo puede ayudarle la seguridad a conseguirlas.

Muestre también el otro lado: cómo puede un incidente de seguridad poner sus planes en riesgo. Por ejemplo, si está a punto de lanzar un nuevo producto, ¿cuáles son los posibles daños para su empresa de que esa propiedad intelectual se haga pública o se destruya?

De hecho, no tiene que ser un problema hipotético. Si puede cuantificar de qué forma los problemas de seguridad existentes ya le están costando a su negocio, entonces eso le da un argumento aún mejor.

Repetir, repetir, repetir

Es poco probable que obtenga todo lo que necesita de una única conversación. Haga su comunicación simple y frecuente. Establezca actualizaciones periódicas e informe con frecuencia sobre las métricas pertinentes. No tenga miedo de repetir y probar unos cuantos ángulos diferentes hasta que el mensaje cale y consiga los fondos y el apoyo que necesita.

Cómo le ayudará el GDPR

En muchos casos, los profesionales de la seguridad tienen problemas para hablar el mismo idioma que su junta directiva y ayudarles a entender por qué necesitan dar prioridad a la inversión en seguridad. Cuando un ataque cibernético público ocurre y los ejecutivos ven el daño multidimensional que causa, entonces esos motivos para invertir se vuelven muy claros. Las conversaciones (y los cambios) ocurren a un ritmo mucho más rápido cuando todos entienden el problema.

Aquí es donde leyes tales como el Reglamento general sobre la protección de datos (GDPR), que entró en vigor en mayo de 2018, pueden ayudar a mejorar la seguridad.

Las empresas que ya están invirtiendo en seguridad pueden no tener mucho de qué preocuparse, ya que probablemente vayan por buen camino para cumplir con la ley (en el aspecto de la seguridad del GDPR). Por otro lado, para aquellas organizaciones que han estado luchando para obtener fondos para invertir, el GDPR ofrece una gran oportunidad para que los profesionales de la seguridad y los principales líderes de la seguridad estén en la misma sintonía. Las nuevas legislaciones como ésta están obligando a las empresas a cumplir unas normas mínimas, lo que ayudará a respaldar una mayor innovación tecnológica en el futuro.

La privacidad de datos y seguridad de TI no solo son requisitos normativos, sino también demandas del cliente. Cada vez es más frecuente que las empresas reciban preguntas de sus clientes sobre cómo están manejando sus datos. Hay una relación de confianza, una suposición de que la empresa que recibe sus datos se preocupará por ellos. La ley solo está ahí para garantizar que las empresas hagan todo lo posible por respetar esa confianza.

Proteja su negocio con Cisco

Seguridad de la red

¿Qué es la seguridad de la red?
La seguridad de la red es cualquier actividad diseñada para proteger la usabilidad e integridad de su red y de sus datos. Incluye las tecnologías de hardware y software. La seguridad efectiva de la red administra el acceso a la red. Va dirigida a distintas amenazas y evita que entren o que se propaguen en la red.

¿Cómo funciona la seguridad de la red?
La seguridad de la red combina varios niveles de defensas en el perímetro y en la red. Cada nivel de seguridad de la red implementa políticas y controles. Los usuarios autorizados obtienen acceso a los recursos de la red, pero impide que los agentes maliciosos lleven a cabo explotaciones y amenazas.

¿Cómo me beneficio de la seguridad de la red?

La digitalización ha transformado nuestro mundo, la forma en la que vivimos, trabajamos, jugamos y aprendemos. Cada organización que desee ofrecer los servicios que los clientes y empleados exigen debe proteger su red y su información confidencial de los ataques. En última instancia, protege su reputación.

6 medidas que puede adoptar para proteger su red

1. Supervise el tráfico entrante y saliente de su firewall y lea los informes cuidadosamente. No dependa de alertas para identificar una actividad peligrosa. Asegúrese de que alguien de su equipo comprende los datos y está preparado para tomar las medidas necesarias.
2. Esté atento a las nuevas amenazas a medida que se detectan y se publican en línea. Por ejemplo, el blog de Cisco Talos proporciona actualizaciones instantáneas sobre nuevas amenazas, vulnerabilidades y un resumen semanal detallado de las amenazas. La página TrendWatch de Trend Micro realiza un seguimiento de la actividad actual de las amenazas. Además, puede hacer que el Equipo de Respuesta ante Emergencias Informáticas de EE. UU. (US-CERT, una división de Seguridad Nacional) le envíe alertas por correo electrónico sobre explotaciones y vulnerabilidades de software recientemente confirmadas.
3. Habilite las actualizaciones periódicas para su software del firewall y del antivirus.
4. Forme a los empleados de manera continua para que comprendan cualquier cambio en su política de uso aceptable. Además, fomente un enfoque de “vigilancia vecinal” de la seguridad. Si un empleado nota algo sospechoso, como que no puede iniciar sesión en una cuenta de correo electrónico de inmediato, debe notificárselo a la persona adecuada inmediatamente.
5. Instale una solución de protección de datos. Este tipo de dispositivo puede proteger a su empresa contra la pérdida de datos si se vulnera la seguridad de su red.
6. Tenga en cuenta soluciones de seguridad adicionales que protegerán aún más su red y ampliarán las capacidades de su empresa.

Tipos de seguridad de red

Control de acceso

No todos los usuarios deben tener acceso a su red. Para mantener alejados a los posibles atacantes, necesita reconocer a cada usuario y a cada dispositivo. A continuación, puede aplicar sus políticas de seguridad. Puede bloquear los dispositivos de terminales no conformes o darles un acceso limitado. Este proceso es el control de acceso a la red (NAC).

Seguridad de la aplicación

Cualquier software que utilice para llevar su negocio necesita estar protegido, ya sea que su personal de TI lo construya o lo compre. Por desgracia, cualquier aplicación puede contener agujeros o vulnerabilidades que los atacantes pueden utilizar para infiltrarse en su red. La seguridad de las aplicaciones abarca el hardware, el software y los procesos que utiliza para cerrar esos huecos.

Software antivirus y antimalware

El “malware”, la abreviatura de “software malicioso”, incluye los virus, los gusanos, los troyanos, el ransomware y el spyware. A veces, el malware infecta una red pero permanece inactivo durante días o incluso semanas. Los mejores programas antimalware no solo buscan malware en el momento de la entrada, sino que también realizan un seguimiento continuo de los archivos después para detectar anomalías, eliminar el malware y reparar los daños.

Prevención de la pérdida de datos

Las organizaciones deben asegurarse de que su personal no envía información confidencial fuera de la red. Las tecnologías de prevención de pérdida de datos, o DLP, pueden impedir que las personas carguen, reenvíen o incluso impriman información importante de forma insegura.

Análisis de comportamiento

Para detectar el comportamiento anormal de la red, debe saber lo que es un comportamiento normal. Las herramientas de análisis de comportamiento diferencian automáticamente las actividades que se desvían de la norma. Su equipo de seguridad puede entonces identificar mejor los indicadores de compromiso que plantean un problema potencial y remediar rápidamente las amenazas.

Seguridad para el correo electrónico

Los gateways de correo electrónico son el vector de amenaza número uno para una violación de la seguridad. Los atacantes utilizan información personal y tácticas de ingeniería social para crear sofisticadas campañas de suplantación de identidad para engañar a los destinatarios y enviarlos a sitios que ofrecen malware. Una aplicación de seguridad para el correo electrónico bloquea los ataques entrantes y controla los mensajes salientes para evitar la pérdida de datos confidenciales.

Firewalls

Los firewalls levantan una barrera entre la red interna fiable y las redes externas no fiables, como Internet. Usan un conjunto de reglas definidas para

permitir o bloquear el tráfico. Un firewall puede ser hardware, software o ambos. Cisco ofrece dispositivos de Unified Threat Management (UTM) y firewalls de última generación centrados en las amenazas.

Sistemas de prevención de intrusiones

Un sistema de prevención de intrusiones escanea el tráfico de red para bloquear los ataques de forma activa. Los appliances de IPS de última generación de Cisco hacen esto correlacionando grandes cantidades de inteligencia sobre amenazas globales, no solo para bloquear las actividades maliciosas, sino para rastrear el progreso de archivos sospechosos y malware en la red y así evitar que se extiendan brotes o que se produzcan infecciones de nuevo.

Seguridad de dispositivos móviles

Los ciberdelincuentes se centran cada vez más en las aplicaciones y los dispositivos móviles. Dentro de 3 años, puede que el 90 % de las organizaciones de TI apoyen las aplicaciones empresariales en los dispositivos móviles personales. Es evidente que necesita controlar qué dispositivos pueden acceder a su red. También tendrá que configurar sus conexiones para que el tráfico de red sea privado.

Segmentación de red

La segmentación definida por software clasifica el tráfico de red en diferentes categorías y hace que sea más fácil hacer cumplir las políticas de seguridad. De forma ideal, la clasificación está basada en la identidad del terminal, no simplemente en las direcciones IP. Puede asignar derechos de acceso basados en el rol, y la ubicación, entre otros, para hacer que el nivel correcto de acceso se conceda a la gente correcta y para que los dispositivos sospechosos se contengan y se reparen.

VPN

Una red privada virtual cifra la conexión de un terminal a una red, a menudo a través de Internet. Normalmente, una VPN de acceso remoto usa IPsec o capa de conexión segura para autentificar la comunicación entre el dispositivo y la red.

Seguridad web

Una solución de seguridad web controlará el uso que el personal hace de la web, bloqueará las amenazas basadas en la web y negará el acceso a los sitios web maliciosos. Protegerá el gateway web del sitio o de la nube. “Seguridad web” también se refiere a los pasos que adopta para proteger su propio sitio web.

Seguridad inalámbrica

Las redes inalámbricas no son tan seguras como las redes por cable. Sin medidas de seguridad rigurosas, instalar una LAN inalámbrica puede ser como poner puertos Ethernet en todas partes, incluso en el aparcamiento. Para evitar que la gente se aproveche de la red, necesita productos diseñados específicamente para proteger la red inalámbrica.

Inteligencia de amenazas de Talos

Talos es un equipo de inteligencia y de investigación de amenazas de Cisco líder en el sector, y cada producto de seguridad de Cisco se protege a través de Talos. Talos tiene más de 250 investigadores de amenazas que trabajan

ininterrumpidamente y en todo el mundo, con un repositorio de 100 terabytes de inteligencia de amenazas.

Vemos una tercera parte del tráfico de correo electrónico mundial y un 2 % de las solicitudes DNS del mundo. Nos encontramos con 1,1 millones de muestras de malware únicas cada día a través de nuestra protección frente a malware avanzado y tecnología Threatgrid, que nos permiten bloquear 19 700 millones de amenazas en un día en las redes de nuestros clientes.

Eso es 19 700 millones de amenazas bloqueadas al día.

Ese conocimiento inmenso y esas capacidades de investigación respaldan las soluciones de ciberseguridad de Cisco, que ofrecen la visibilidad, automatización, flexibilidad y escalabilidad obligatorios para proteger el entorno de su red contra las amenazas sofisticadas que están en aumento.

Cisco Umbrella

Un servicio de seguridad en la nube que ofrece protección integrada para su servicio de Internet.

Cisco Umbrella es un servicio de seguridad en la nube que ofrece protección integrada contra los ataques en su conexión de Internet, ayudándole a atenuar el tiempo y el coste que se gasta en los ciberataques.

La solución ofrece la protección proactiva contra las amenazas de Internet, como el malware, la botnet y las suplantaciones de identidad. Ayuda a que su empresa esté segura, ya que ofrece un tráfico limpio antes de que llegue a su red interna, pues utiliza de forma efectiva la ubicación de las etapas de los ataques, y bloquea las amenazas en todos los puertos y protocolos. Puede estar convencido de que con el acceso a Internet seguro, está protegido con una primera capa de defensa contra el malware.

Cisco Umbrella ofrece visibilidad a todas las solicitudes de Internet de su red, de cada puerto, protocolo o aplicación para detectar y bloquear conexiones de dominios maliciosos e IP. Vea por qué las pequeñas empresas se están dando cuenta del efecto multiplicador de la seguridad mediante el uso de DNS para complementar medidas de seguridad existentes. ¿Qué ataques no ve?

Firewall de última generación

Un firewall tradicional puede controlar el tráfico a la entrada o la salida de una red. En otras palabras, es el puente levadizo entre su propia empresa y la “gran parte no fiable” del resto de Internet.

Esto era perfecto en aquellos tiempos sencillos, cuando podía ver todo lo que se aferraba a su red. Ahora, las empresas están empezando a jugar cada vez más el papel de anfitrión para un número de dispositivos desconocidos y un mar oscuro y profundo de aplicaciones en la nube que descargan los empleados.

La principal diferencia con el firewall de última generación es que puede establecer controles y políticas de aplicaciones. Por ejemplo, si un miembro de sus plantilla descarga un software de uso compartido de archivos que quizás no sea seguro, esto se hará visible de forma automática y podrá reaccionar de forma inmediata.

Además, lo más importante es que ganará mucha más visibilidad y control de los usuarios, dispositivos, amenazas y vulnerabilidades en su red. Por lo tanto, cuando su junta directiva le pregunte, "¿Estamos seguros?", puede ofrecer una respuesta mucho más amplia que en el caso de que tuviera un firewall tradicional que solo controlara el tráfico.

Obtenga más información sobre firewalls de última generación o encuentre el mejor Firewall de última generación para usted.

Protección frente a malware avanzado

Seguridad para terminales de última generación

La seguridad para terminales de última generación es la integración de la prevención, la detección y la respuesta de las capacidades de una sola solución, aprovechando el poder de los análisis basados en la nube. Cisco AMP para terminales es un conector ligero que funciona con tus dispositivos Windows, Mac, Linux, Android e iOS.

Cisco AMP para terminales ofrece una protección exhaustiva contra los ataques más avanzados. Evita las brechas y bloquea el malware en el punto de entrada; a continuación detecta, contiene y soluciona de forma rápida amenazas avanzadas que evaden las defensas de primera línea y se introducen en su red.

Evita: aumenta las defensas utilizando la mejor inteligencia de amenazas global y bloquea el malware basado en archivos o no en tiempo real.

Detecta: supervisa y registra de forma continua la actividad de todos los archivos para detectar rápidamente el malware sigiloso.

Responde: acelera las investigaciones y remedia de forma automática el malware en ordenadores, servidores Mac, Linux y dispositivos móviles (Android e iOS).

Puede utilizar la nube pública o se puede desarrollar como una nube privada. AMP supervisa y analiza de forma continua todos los archivos y la actividad de los procesos de su red para descubrir el 1 por ciento de las amenazas que otras soluciones pasan por alto. AMP nunca pierde de vista dónde va un archivo o lo que hace. Si un archivo que parece limpio en una inspección inicial alguna vez muestra un comportamiento malicioso, AMP está ahí con un historial completo del comportamiento de las amenazas para detectar, contener y solucionar.

Detección de amenazas desconocidas

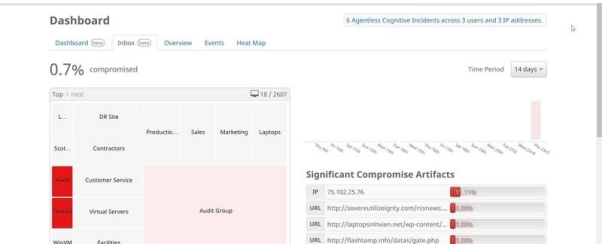
La tecnología de sandboxing integrada de AMP analiza el comportamiento de los archivos sospechosos y establece una correlación frente a otras fuentes de información. El análisis de archivos genera información detallada para ofrecerle una información más precisa de cómo contener el brote y bloquear los futuros ataques.

Cuando un archivo se considera malicioso, AMP reduce drásticamente la cantidad de tiempo y de recursos necesarios para investigar. Proporciona información de forma automática sobre las cuestiones más urgentes, incluidas:

- ¿Qué ha ocurrido?
- ¿De dónde proviene el malware?
- ¿Dónde ha estado el malware?
- ¿Qué está haciendo ahora el malware?
- ¿Cómo lo detenemos?

Con unos pocos clics en la consola de gestión basada en navegador de AMP, se puede bloquear el archivo para que no pueda ejecutarse en ningún terminal. Cisco AMP sabe en qué otros terminales ha estado el archivo, de modo que se puede poner en cuarentena para todos los usuarios. Con AMP, la corrección del malware es quirúrgica y no produce daños colaterales asociados a los sistemas de TI o en la empresa.

Cómo detener y poner en cuarentena un archivo con Cisco AMP:



Cisco Meraki

Seguridad gestionada en la nube y SD-WAN

Una administración centralizada 100 % en la nube para controlar la seguridad, el networking y las aplicaciones.

Los appliances de seguridad de Cisco Meraki se pueden implementar de forma remota en cuestión de minutos, utilizando el aprovisionamiento de nube sin intervención. La configuración de seguridad es fácil de sincronizar en miles de sitios a través de plantillas. La tecnología de seguridad VPN conecta las sucursales en tres clics, mediante un panel intuitivo basado en la web.

Seguridad completa en un solo dispositivo

Cada appliance de seguridad de Meraki admite varias características, como un stateful firewall y un motor de prevención de intrusiones SourceFire integrado, para mantener seguras las redes. Las listas de filtros y de definiciones de amenazas se actualizan sin contratiempos, garantizando que cada sitio cuenta con la máxima protección de las últimas vulnerabilidades y los sitios web problemáticos.

Proteger un sitio en cuestión de minutos

1. Agregue el appliance de seguridad Meraki al panel.
2. Active la prevención de intrusiones.
3. Seleccione el nivel de protección contra amenazas que desee.

Más información

Para consultar las últimas innovaciones y perspectivas, visite: Cisco Tech Connection para pymes o descubra más de los recursos para pymes de Cisco y de la seguridad de Cisco para proteger su empresa.

Gracias por leer esta información

Elementos esenciales de seguridad en las pymes