HORNETSECURITY

INFO
SHEET

SECURITY AWARENESS SERVICE

REFUERZA LA SEGURIDAD DE TU CADENA DE SUMINISTRO

En este informe, exploramos las vulnerabilidades presentes en las cadenas de suministro y cómo fomentar una cultura sólida de seguridad mediante una formación continua en concienciación es esencial para proteger los datos tanto de los proveedores de servicios como de las empresas a las que sirven.

PANORAMA DE RIESGOS EN LA CADENA DE SUMINISTRO

Las organizaciones actuales dependen de una amplia gama de componentes de hardware, aplicaciones de software y servicios en la nube, todos ellos proporcionados por múltiples proveedores. Esta interdependencia crea varios puntos de riesgo:

- **Redes Complejas de Proveedores:** Cada proveedor, ya sea de componentes físicos o de software, representa una posible puerta de entrada para un ataque.
- **Phishing e Ingeniería Social:** Los atacantes suelen emplear métodos sofisticados de phishing para comprometer a los proveedores y, posteriormente, atacar a sus clientes.compromise vendors and then target their clients.

EJEMPLOS REALES

Ataques al NHS y Change Healthcare

Interrupciones en servicios críticos han tenido un impacto generalizado. Los ataques recientes de ransomware (Synnovis) paralizaron los diagnósticos del NHS e interrumpieron masivamente las operaciones de Change Healthcare.

Incidente de SolarWinds

Una brecha de alto perfil que demostró cómo las actualizaciones comprometidas pueden otorgar a los atacantes acceso a redes que, de otro modo, serían seguras. Una brecha de alto perfil que demostró cómo las actualizaciones comprometidas pueden dar a los atacantes acceso a redes que, de otro modo, serían seguras. La inteligencia rusa alteró una actualización de SolarWinds Orion, infiltrándose en muchas organizaciones a través de un parche malicioso.

3CX en North Korea

Los hackers norcoreanos ejecutaron un ataque de varias etapas en 2023, comprometiendo 3CX a través de software de terceros en el PC de un empleado. Esto permitió la distribución global de una actualización maliciosa de 3CX.

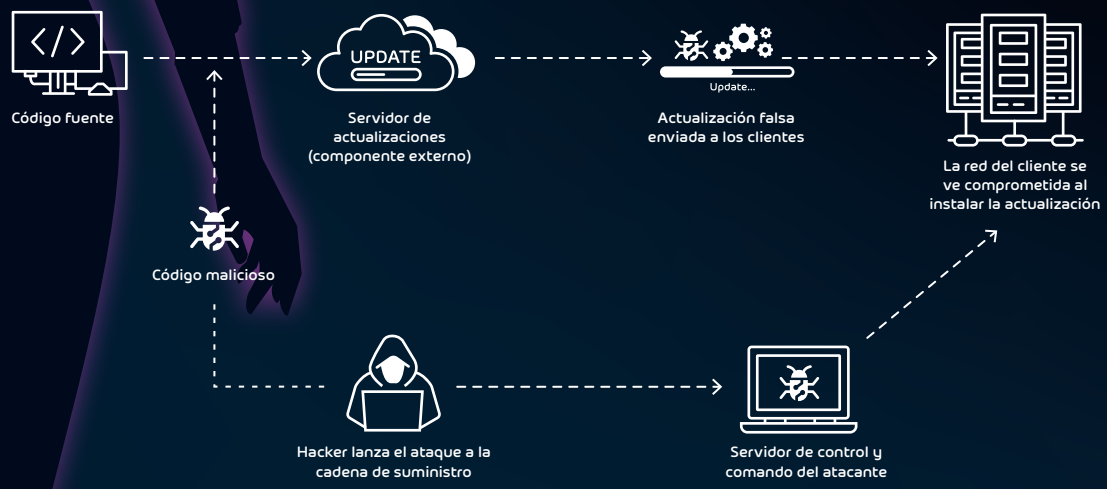
HORNETSECURITY

INFO
SHEET

ANATOMÍA DE UN ATAQUE A LA CADENA DE SUMINISTRO

Entender cómo funcionan estos ataques es clave para poder prevenirlos:

- **Comprometen al proveedor:** Los atacantes se infiltran en un proveedor de confianza, aprovechando dependencias o sistemas de actualización de terceros.
- **Insertan un código malicioso:** Una vez dentro, insertan software malicioso que les abre la puerta a otros sistemas.
- **Distribuyen la amenaza:** La actualización contaminada llega a los clientes del proveedor, comprometiendo sus sistemas sin que lo sepan.
- **Robo de datos e interrupciones:** Con acceso a las empresas objetivo, los atacantes pueden robar información sensible y paralizar operaciones clave.



LA CONCIENCIACIÓN EN SEGURIDAD NO ES OPCIONAL

Cuando se trata de cadenas de suministro, no solo está en juego la seguridad del proveedor. Si un eslabón falla, todas las empresas conectadas pueden verse afectadas. Y por muy buenas que sean tus defensas técnicas, un simple error humano puede tirar todo por la borda. La ciberresiliencia no se basa solo en la tecnología; se construye con personas. Por eso es esencial:

- **Formar al equipo:** Enseña a tus empleados a detectar intentos de phishing y engaños. Son tu primera línea de defensa.
- **No parar nunca:** La formación debe ser continua y adaptarse al ritmo de las nuevas amenazas. Si tus empleados están bien preparados, evitarás más de un susto.

09-25

HORNETSECURITY

INFO
SHEET

SECURITY AWARENESS SERVICE: TU ESCUDO FRENTE A LAS AMENAZAS EN LA CADENA DE SUMINISTRO

El Security Awareness Service de Hornetsecurity está pensado para cerrar la brecha entre las defensas técnicas y los fallos humanos mediante:

- **Employee Security Index (ESI):** Evalúa el perfil de riesgo de cada persona y adapta la formación a lo que realmente necesita.
- **Formación continua automatizada:** Simulacros de phishing frecuentes y contenido educativo para mantener alerta al personal y que no baje la guardia.
- **Sin complicaciones:** Se integra fácilmente con tus sistemas de seguridad actuales, aliviando la carga de trabajo del equipo y reforzando la protección.
- **Resultados que se notan:** Una cultura de seguridad sólida reduce los incidentes de phishing y los ataques de ingeniería social, protegiendo toda la cadena de suministro.

VENTAJAS CLAVE

Menos exposición:

Anticípate a los riesgos formando a tu equipo sobre amenazas actuales.

Relaciones más fuertes con tus proveedores

Demostrar que te tomas en serio la seguridad genera confianza.

Preparados para lo que venga:

Asegura la continuidad del negocio incluso ante ataques complejos.

Un plus frente a la competencia

Contar con un equipo bien formado marca la diferencia en el mercado.

Forma a tu equipo y conviértelo en la primera línea de defensa contra las ciberamenazas.

¡DESCUBRE MÁS!

09/25