LITORALPRESS

Fecha: 03-07-2025
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: **Cuando la prevención se transforma en vigilancia: ciberresiliencia activa**

Pág. : 17
Cm2: 283,2
VPE: $ 2.509.219

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

Cuando la prevención se transforma en vigilancia: ciberresiliencia activa

nlt.secure

Cerramos nuestro primer pilar: la **prevención**. Una etapa que no termina, sino que se transforma en la base sobre la que construiremos detección, respuesta y recuperación.

En **NLT Secure** entendemos que la ciberresiliencia no es un estado estático, sino un proceso continuo y estratégico que permite a las organizaciones protegerse, operar y crecer incluso en medio de amenazas constantes.

Durante estos meses hemos trabajado juntos el Pilar de **Prevención**, que abarca cuatro dimensiones esenciales:

1. Diagnóstico de red y TI: conocer antes de proteger

Sin visibilidad, no hay seguridad. Realizar un diagnóstico exhaustivo de la infraestructura permite identificar brechas, vulnerabilidades y configuraciones que podrían convertirse en puertas de entrada para los atacantes.

Ejemplos clave:

- Simulación de ataques controlados (red teaming, adversary simulation)
- Pruebas de penetración (pentesting) orientadas a identificar vulnerabilidades reales
- Análisis de vulnerabilidades con priorización de riesgos

Por qué es clave:

Permite a los líderes tomar decisiones informadas y dirigir sus recursos a los puntos de mayor impacto y exposición real.

2. Planificación estratégica de la seguridad

Con el diagnóstico como base, la planificación define cómo proteger la organización de forma alineada al negocio y a los marcos regulatorios vigentes, como la nueva Ley Marco de Ciberseguridad. Esta etapa traduce resultados técnicos en un camino claro hacia la resiliencia.

Ejemplos clave:

- Servicios de vCISO (CISO virtual) para diseñar y liderar la estrategia de seguridad
- Construcción de Planes de Continuidad Operacional (BCP) y Recuperación ante Desastres (DRP)
- Diseño de programas de cumplimiento normativo y madurez de seguridad

Por qué es clave:

Sin planificación, las acciones se vuelven reactivas, costosas y fragmentadas. Una estrategia bien definida asegura coherencia, eficiencia y cumplimiento.

3. Fortalecimiento de controles: proteger para operar

Aquí pasamos de la teoría a la acción. Implementamos tecnologías y procesos que protegen el perímetro, las redes, la nube, los dispositivos, los accesos y los datos.

Ejemplos clave:

- Firewalls NGFW, SD-WAN, ZTNA, WAF y seguridad OT con Fortinet
- Protección de endpoints con EDR y XDR, y **prevención** de fugas con DLP
- Remediación automatizada de vulnerabilidades con inteligencia artificial (Vicarius)

Por qué es clave:

La protección no puede quedarse en buenas intenciones o políticas en papel. Debe traducirse en herramientas que bloqueen ataques, mitiguen vulnerabilidades y aseguren continuidad operativa.

4. Concientización y formación: las personas como primera línea de defensa

Ninguna tecnología es suficiente si las personas no están preparadas. La concientización transforma la cultura organizacional, reduce errores humanos y fortalece la respuesta ante phishing, ingeniería social y malas prácticas digitales.

Ejemplos clave:

- Simulaciones de phishing con métricas de aprendizaje
- Programas de concientización adaptados a cada rol
- Formación en mejores prácticas y políticas de seguridad

Por qué es clave:

Más del 80% de los incidentes de ciberseguridad comienzan con un error humano. Invertir en personas es proteger los cimientos de la organización.

Una ciberresiliencia viva: prevenir, detectar y responder

Con estos cuatro pasos completados, tu organización no solo está protegida. Está lista para dar el siguiente paso: la detección proactiva y la respuesta inmediata ante amenazas activas.

Porque la ciberresiliencia real es un ciclo:

1. Diagnosticar y prevenir
2. Detectar y responder
3. Recuperar y fortalecer

En las próximas semanas abordaremos nuestro segundo pilar: Detección y Respuesta. Exploraremos cómo soluciones como CyberSpectrum MDR, Inteligencia de Amenazas y **Prevención** de Fraude Digital pueden convertirse en los ojos y oídos de tu negocio, anticipándose a los atacantes y asegurando la continuidad de tus operaciones.

Contáctanos:

Email: hello@nltsecure.com
Teléfono: +56 22 399 4300
WhatsApp: +1 321 732 1664

NLT SECURE: Building a safer digital world for everybody, together!

Conoce más en:
www.nltsecure.com