PRONTOCYBER®
BY CY4GATE

Respuesta digital de emergencia ante incidentes de ciberseguridad

Libro Blanco

Libro Blanco

CY4GATE

Rev. núm. 1 de 08/08/2022

PRONTOCYBER®
BY CY4GATE

Resumen

PRONTOCYBER®
BY CY4GATE

1 Servicio de Emergencia Digital

1.1 Ciberconsultoría

La intervención cibernética de emergencia permite a los clientes recibir ayuda inmediata en caso de violación de la ciberseguridad.

El servicio lo prestan recursos con competencias y conocimientos específicos en el ámbito de la gestión de incidentes de seguridad y con experiencia en Respuesta a Incidentes, incluso en realidades complejas.

Para apoyar y garantizar una respuesta correcta y rápida en caso de incidentes y/o ataques hostiles, se adopta un proceso conforme a la norma ISO/IEC 27035, consolidado y enriquecido por muchos años de experiencia en CERT.

Pronto Intervento Cyber también permite, cuando sea necesario, apoyar, y si es necesario, coordinar, las actividades necesarias para restablecer el correcto funcionamiento de los servicios afectados por el incidente.

Preparados para la ciberintervención - Objetivos:

- Detectar rápidamente una infracción e identificar las estrategias de respuesta más adecuadas.
- Reducir significativamente los tiempos de respuesta y los daños causados.
- Recopilar la información necesaria para apoyar posibles acciones legales.
- Proteger la reputación y los activos del cliente.
- Evaluar las implicaciones de las mejores prácticas del sector y la normativa vigente (privacidad, etc.).
- Analizar el incidente ocurrido identificando errores, puntos débiles y estrategias adoptadas para su gestión, mejorando la respuesta ante futuros incidentes.

Ciberintervención de urgencia - Incidentes atendidos:

- **PERSISTENCIA**
- **MAYORES PRIVILEGIOS**
- **EVITAR LA DEFENSA**
- **ACCESO A LAS CREDENCIALES**
- **DESCUBRIMIENTO**
- **MOVIMIENTO LATERAL**
- **EJECUCIÓN**
- **RECOPILACIÓN**
- **EXFILTRACIÓN**
- **MANDO Y CONTROL**
- **DENEGACIÓN DE SERVICIO (DOS)**

1.2 Aviso legal

Legal First Aid permite a los clientes recibir asistencia jurídica inmediata en caso de violación de la seguridad.

El servicio lo prestan recursos experimentados con competencias y conocimientos específicos en el ámbito de la gestión jurídica de incidentes de seguridad.

El servicio se activará a raíz de una violación de la seguridad que entre en las siguientes categorías:

- una violación de la confidencialidad, es decir, cuando se produce una divulgación no autorizada o accidental de datos personales o se accede a ellos;
- una violación de la disponibilidad, es decir, cuando se produce una pérdida, inaccesibilidad o destrucción, accidental o no autorizada, de datos personales;
- una violación de la integridad de la información, es decir, cuando se produce una alteración no autorizada o accidental de datos personales. Este tipo concreto de incumplimiento también cubre los casos de indisponibilidad temporal.

En el plazo de 36 horas desde el primer contacto, los expertos jurídicos evaluarán el alcance de la violación de datos en términos de su impacto sobre los datos personales y los derechos y libertades de los interesados; determinarán si ha habido o no violación de datos personales.

PRONTOCYBER®
BY CY4GATE

2 Ciberevaluación

Una correcta gestión de la seguridad se basa principalmente en un conocimiento adecuado del nivel actual de protección de los propios sistemas.

Teniendo esto en cuenta, un programa de seguridad y auditoría debe incluir la actividad combinada de Evaluación de Vulnerabilidades (VA) y Pruebas de Penetración (PT), que ayudan a comprender el nivel real de seguridad de los procesos corporativos propios.

2.1 Evaluación de la vulnerabilidad

La Evaluación de Vulnerabilidades (VA) proporciona una lista de las vulnerabilidades más inmediatamente identificables y, a continuación, mitigarlos priorizando y estructurando las medidas correctoras.

La actividad de VA, de hecho, tiene como objetivo llevar a cabo una evaluación dinámica del nivel de seguridad de los dispositivos conectados a la red interna o externa y de los servicios y aplicaciones web expuestos al mundo exterior, con el fin de identificar cualquier vulnerabilidad relacionada con posibles errores de configuración de la seguridad, falta de niveles de protección activos, software obsoleto, dispositivos no autorizados dentro de la red, etc., que puedan exponer el sistema de información corporativo a riesgos de violación.

El principal objetivo de la VA es verificar los niveles de seguridad y eficacia de los activos identificados, detectar posibles criticidades y proponer las consiguientes medidas correctoras para garantizar la aplicación de las mejores características de seguridad y fiabilidad del sistema en uso.

Las evaluaciones de vulnerabilidad, por tanto, son un verdadero análisis de todos los activos informáticos de la empresa, esenciales para identificar y clasificar los riesgos y vulnerabilidades. La cartografía de toda la infraestructura informática permite poner de relieve los puntos críticos potenciales y, a continuación, aplicar las medidas de prevención y protección necesarias para el sistema informático.

2.2 Pruebas de penetración

El servicio de Evaluación Cibernética proporciona una verificación dinámica de la seguridad de los sistemas del Cliente con el fin de identificar cualquier vulnerabilidad, configuración de seguridad incorrecta y deficiencias en los niveles de protección activa que expongan el contexto a ataques externos. La metodología adoptada hace referencia a la norma internacional para la ejecución de pruebas de seguridad elaborada por ISECOM y a las directrices para las actividades de evaluación de aplicaciones definidas por OWASP.

Basándose en la experiencia acumulada, los principios de ISECOM se han agrupado y reorganizado en un proceso probado que también incluye algunos conceptos innovadores tanto en la clasificación de vulnerabilidades como en la representación de problemas y áreas de intervención, como se describirá en las siguientes secciones.

El objetivo de una Evaluación de Seguridad, por tanto, es recopilar el conjunto de información que puede dar lugar a la interrupción de un servicio o a la intrusión en los sistemas del Cliente, trabajando con una metodología tomada de la utilizada habitualmente por los hackers a través de pruebas específicas (intrusivas y no intrusivas).

El servicio implica un análisis y una identificación en varias etapas de las vulnerabilidades de seguridad, utilizando no solo una lógica operativa basada en el uso de herramientas automatizadas, sino también mediante operaciones de verificación y ataque racionalizadas por miembros de un equipo altamente especializado con conocimientos específicos.

El equipo ha adoptado una metodología personalizada sustentada en un subconjunto de pruebas basadas en partes de la metodología OSSTMM (Open Source Security Testing Methodology Manual), complementada con un proceso de validación orientado al negocio para garantizar la ejecución de una evaluación adecuada de cada criticidad y modulando el método en relación con la tecnología específica considerada y las necesidades concretas del cliente.

PRONTOCYBER®
BY CY4GATE

3 Concienciación cibernética

3.1 Cibereducación

El objetivo de la formación es concienciar a los participantes sobre los riesgos de la ciberseguridad, con especial atención a los distintos ámbitos de la seguridad.

El programa de formación sobre concienciación en ciberseguridad, impartido en italiano, adopta la forma de un "itinerario de aprendizaje" de 3 horas y 45 minutos y abordará los principales ataques que afectan a las empresas, el reconocimiento de los riesgos de navegar por Internet y las mejores prácticas para moverse por la red con seguridad.

A continuación se presentan algunas estrategias de formación que se adoptarán para el uso de los Itinerarios de aprendizaje/Webinarios:

Webinar con acceso ilimitado;

- Verificación del nivel de partida de los participantes a través de un cuestionario inicial, realizado mediante preguntas cerradas a modo de autoevaluación.
- Combinación del enfoque frontal para transmitir el contenido de la actividad formativa y en modalidad interactiva.
- Intervención de los participantes en el seminario web utilizando contenidos multimedia (vídeos, imágenes, glosarios, artículos del sector) sobre ejemplos de casos reales de ciberataques en contextos empresariales.
- Verificación del aprendizaje mediante la preparación de preguntas cerradas al final del seminario web.
- Expedición de un certificado al finalizar el curso.
- Durante el seminario web habrá espacio para preguntas y consultas relacionadas con los temas tratados durante el curso.

La plataforma de formación será proporcionada por el cliente y se prestará todo el apoyo necesario para la integración de las grabaciones de los seminarios web en la plataforma de formación corporativa existente.

3.2 Campañas de phishing

Teniendo en cuenta que los mayores peligros para la seguridad de las organizaciones residen en los buzones de correo electrónico de empleados y colaboradores, el servicio de simulación de ataques Phishing prevé la ejecución de escenarios reales para poner a prueba y sensibilizar a los usuarios de la empresa.

Las simulaciones de ataques de phishing se personalizan en función de las características particulares de la organización objetivo, y hacen uso de los conocimientos y experiencia del equipo en materia de equipo rojo, equipo azul, ingeniería social y técnicas y tácticas de ciberataque de última generación.

Al final de cada campaña de ataque, se elabora un informe con información detallada puramente orientada al resultado, útil tanto para medir como para reducir los riesgos.

El servicio es un complemento ideal de los programas de formación en sensibilización con el objetivo último de aumentar la capacidad de reacción del individuo, cada vez más expuesto y víctima de este tipo de ataques.

Fases de desarrollo de una campaña de phishing:

- **Fase 1 - Propuesta de campaña de phishing**
- **Paso 2 - Objetivo de aceptación e identificación**
- **Paso 3 - Ejecución de la campaña de phishing**
- **Paso 4 - Presentación de informes**

www.prontocyber.com