SOFISTIC
CYBERSECURITY

Ciberseguridad en centros sanitarios, defendiendo a quienes más nos protegen

¿Por qué el foco de ataques está en los centros sanitarios?

La situación de desprotección del sector sanitario es uno de los mayores problemas que afronta el sector en tiempos de pandemia.

Los ciberataques a los hospitales buscan conseguir recompensas económicas fáciles debido a la presión que supone para estas instituciones tener sus sistemas sin funcionar, lo que **precipita pagar los rescates en muchos casos de ransomware**. Existen también otras motivaciones, como el robo de identidades del equipo médico, la posible venta de información sensible en la darkweb o incluso el acceso directo a la información directa de los pacientes.

En 2020, América Latina sufrió un aumento del 112% en ataques al sector, y en Europa, España se sitúa en segunda posición en la lista, siendo el tercer país de todo el mundo con mayor grado de infección, justo después de Canadá (250%) y Alemania (220%).

Características que facilitan el ataque

Equipos y dispositivos interconectados 24/7

En primer lugar, se trata de centros que tienen una actividad constante (24x7x365) con equipos de gestión y diagnóstico siempre conectados, siendo sistemas con un mayor grado de componentes informatizados. Los centros sanitarios cuentan con una infraestructura muy compleja para poder gestionar la gran variedad de dispositivos y equipos. Además, suelen ser equipos muy longevos que con el paso del tiempo, sus sistemas de seguridad acaban siendo obsoletos.

Falta de capacitación en seguridad informática

El personal de los centros sanitarios, en la mayoría de los casos, no cuenta con la formación adecuada en ciberseguridad que permita impedir ciberataques como los accesos no autorizados o filtración de información. Como en la mayoría de sectores y empresas, el usuario siempre es el eslabón más débil.

Software no actualizado y equipos obsoletos

A menudo, la existencia de distintos tipos de software para la gestión común de información o incluso para la gestión de información diagnóstica, no cuenta con las actualizaciones de seguridad pertinentes o utiliza sistemas operativos sin ningún tipo de mantenimiento.

Según datos de un informe de Forescout en 2019, el 70% de los ordenadores en el sector salud utilizan sistemas operativos sin soporte de mantenimiento, como Windows 7, para el que Microsoft dejó de mantener en soporte en enero de 2020.

Mayor superficie de ataque cada día

El crecimiento exponencial de dispositivos médicos que requieren de conexión a Internet provoca que exista una amplia superficie de ataque en cada centro hospitalario.

Ya en 2019, según datos de una encuesta de IRDETO a más de 700 responsables de seguridad de centros hospitalarios en Estados Unidos, indicaba que el 82% de esos centros ya había sufrido ataques enfocados a este tipo de instalaciones.

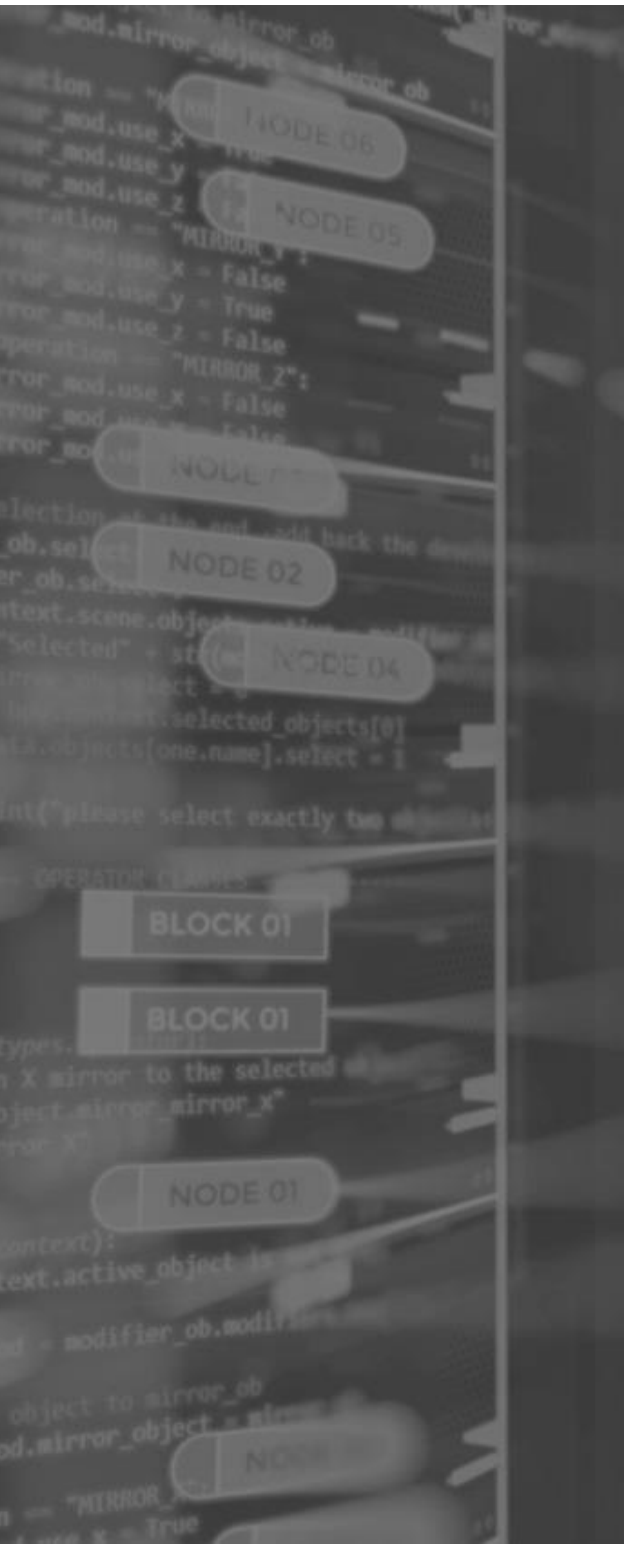
Metodología de Sofistic

Inteligencia artificial frente a ataques 0-day

Gracias a la implementación de plataformas de ciberseguridad con Inteligencia Artificial como Darktrace se consigue obtener visibilidad de todas las posibles amenazas en la red corporativa, respondiendo a las mismas de forma autónoma en tan sólo unos segundos y previniendo que la información se vea comprometida.

Centro de Operaciones de Seguridad ATLANTIS SOC

La combinación del servicio de monitorización 24/7 de Sofistic – Atlantis SOC - con otros herramientas de seguridad permite gestionar de forma centralizada todas las amenazas, dando respuesta con gran rapidez y eficacia. Además, al estar gestionado en dos continentes se consigue mejor eficiencia y mayor contacto con los CSIRT / CERT de cada país.



Aseguramiento de entornos Microsoft y soluciones cloud

Somos especialistas en analizar la implantación de Microsoft365 y adaptamos la plataforma integrando herramientas de ciberseguridad y aplicando configuraciones específicas para que la información esté protegida en todo momento.

En SOFISTIC realizamos un análisis multinivel de la situación de los servicios cloud, analizando posibles defectos de configuración o puertas abiertas, evitando así futuros ataques.

Servicio de consultoría y análisis de vulnerabilidades (pentest)

Gracias a nuestro servicio de pentest, se realiza un análisis minucioso de las brechas de seguridad del cliente (además de defectos de configuración y puertas traseras), obteniendo instrucciones para resolver las incidencias.

EDR, NDR y XDR: Análisis de comportamiento y respuesta autónoma

Es muy importante asegurar los dispositivos de los usuarios, para así evitar posibles vías de ataque. Mediante soluciones EDR (Endpoint Detection and Response) como Crowdstrike y NDR (Network Detection and Response) como Darktrace se obtiene visibilidad a través de todos los dispositivos y de la red, logrando detectar los ciberataques en las etapas más tempranas gracias al apoyo de la Inteligencia Artificial y el Aprendizaje Automático. Así pues, con la combinación de dichas herramientas conseguimos el denominado XDR (Extended Detection and Response), garantizando un mayor nivel de protección al cubrir tanto los dispositivos como la red.

Adicionalmente, podemos hacer uso de soluciones como Exabeam o Sentinel de Microsoft, para recopilar y correlacionar una mayor cantidad de eventos que ocurren en las múltiples capas de seguridad. De esta forma, conseguimos investigaciones más minuciosas para detectar. y responder a ciberataques mucho más sofisticados.