Entrevista con un hacker europeo: "Invertir en ciberseguridad es como un seguro"

A medida que las cosas se vuelven más digitales y todo está conectado, el potencial de un ciberataque crece. Hablamos con Aron Molnar, experto en seguridad de A1 Digital e importante hackers europeos, sobre lo que los minoristas deberían de observar.

Aron Molnar estudió Seguridad Informática en la Universidad de Ciencias Aplicadas, donde participó en varios concursos de hacking. Con su equipo austriaco ganaron el European Cyber Security Challenge. Cuando terminó sus estudios se unió a A1 Telekom. Desde hace tres años trabaja en seguridad en A1 Digital.

P. ¿Cuándo empezaste a analizar la ciberseguridad en el sector de la venta de combustible?

R. El tema de la gasolinera es algo con lo que me tropecé. Al hacer un taller para las industrias en

general sobre cómo deben asegurarse, investigué un poco para obtener ejemplos. Encontré indicadores de tanques automáticos vulnerables en las gasolineras que utilizan motores de búsqueda especiales donde se pueden encontrar dispositivos públicos que no son seguros. Es bastante difícil encontrar dispositivos inseguros debido a la cantidad de honeypots - sistemas que están destinados a ser encontrados y hackeados sólo para ver lo que hacen los atacantes. Este tipo de búsquedas se hacen normalmente a nivel mundial. El producto que encontré fue distribuido en todo el mundo, incluyendo los EE.UU. y Europa.

P. Basándose en su propia investigación, ¿cómo encuentra el nivel de seguridad de la industria del combustible en comparación con otros?

R. No tengo todas las pruebas para responder a esa pregunta. En mi experiencia, hay diferentes tipos de organizaciones. Organizaciones digitales que tienen servicios digitales en su negocio principal. Por lo general, son conscientes de sus riesgos de seguridad y de TI. Hay industrias que tienen altos estándares debido a los requisitos legales, como la banca y la salud. Otras son conscientes de su situación debido a las grandes cantidades de datos que manejan, como una cadena de hoteles. La mayoría de los demás no tienen una presencia digital real y a menudo no son conscientes.

P. La industria de las gasolineras y tiendas de conveniencia se está adaptando rápidamente a las nuevas tecnologías y está cada vez más conectada. ¿A qué cree que los minoristas deberían estar atentos?

R. El problema de la mayoría de las industrias clásicas es que han evolucionado en las últimas décadas con la comunicación en serie, sin autentificación ya que nada estaba conectado; no había necesidad de asegurarla porque había que ir allí, cortar un cable, poner una caja y luego se tenía acceso a ella. A medida que la tecnología evoluciona y los beneficios de la interconexión de sistemas son más claros, algunos dan el paso de interconectar todas las estaciones sin mirar los riesgos. Como las compañías de combustible no tienen el conocimiento en el negocio digital, necesitan confiar en las compañías que sí lo tienen. Son muy dependientes de sus proveedores. Si un proveedor produce una tarjeta de red para una gasolinera, debe tener cuidado y ponerla detrás de un cortafuegos, por ejemplo. Esa es la parte de la industria.

Una cosa muy importante es que sigan las reglas de las medidas clásicas de seguridad informática: tener un sistema antivirus, un sistema de seguridad de correo, segregar los sistemas de pago. Estos jugadores tienen los problemas tradicionales en torno a Windows, correos electrónicos, teléfonos móviles... Además de la parte de la industria. Los sistemas deben ser segregados.

P. Algunos minoristas a cargo de una red más pequeña de sitios pueden pensar que no vale la pena tener un consultor de IT o invertir en un sistema seguro.

R. Es un cálculo fácil de hacer. Una agencia de marketing con 200 empleados fue golpeada por una campaña de rescate y no pudo trabajar durante dos semanas - hay que calcular cuánto cuesta tener a tanta gente sin trabajar. Si el empleado medio cuesta 3.000 euros al mes, 150 euros al día, para

200 empleados que estarían pagando 300.000 euros por dos semanas sin trabajar. Si se añaden las penalizaciones por no poder entregar el combustible o que algunos productos caduquen, se puede añadir eso a los costes. Calcule el daño y divídalo por 10 - esa puede ser la cantidad a invertir en seguridad.

P. Si usted fuera un hacker que buscara penetrar en una red de venta de combustible, ¿qué estaría buscando y cómo podría interrumpirla?

R. Desde la perspectiva de un atacante, siempre se trata de lo que quiero lograr. La mayoría de los atacantes lo hacen sólo por diversión. Volviendo a los medidores de tanques automáticos que encontramos en Internet, muchos atacantes sólo manipularon los nombres del combustible para mostrar que estaban allí. A menudo no debes esperar mucho daño de ellos. Luego están los criminales en busca de dinero, el clásico ataque de rescate. Buscan interrumpir el servicio para obtener un rescate. Esto es algo que se puede hacer a escala, por eso funciona. Un rescate puede ser enviado a un millón de destinatarios, algunos harán clic, otros no. A nivel de país, podemos ver incidentes como el de Ucrania, por ejemplo, donde los hackers causaron un apagón. Podrían modificar los sistemas en Internet para que los operadores de los sitios y los depósitos de combustible no sean notificados cuando el almacenamiento es bajo. Puedes tener hacking político, como un grupo ambientalista radical o un país.

P. Si fueras un hacker buscando penetrar en una red de venta de combustible, ¿qué estarías buscando y cómo podrías interrumpirla?

Desde la perspectiva de un atacante, siempre se trata de lo que quiero lograr. La mayoría de los atacantes lo hacen sólo por diversión. Volviendo a los medidores de tanques automáticos que encontramos en Internet, muchos atacantes sólo manipularon los nombres del combustible para mostrar que estaban allí. A menudo no debes esperar mucho daño de ellos. Luego están los criminales en busca de dinero, el clásico ataque de rescate. Buscan interrumpir el servicio para obtener un rescate. Esto es algo que se puede hacer a escala, por eso funciona. Un rescate puede ser enviado a un millón de destinatarios, algunos harán clic, otros no. A nivel de país, podemos ver incidentes como el de Ucrania, por ejemplo, donde los hackers causaron un apagón. Podrían modificar los sistemas en Internet para que los operadores de los sitios y los depósitos de combustible no sean notificados cuando el almacenamiento es bajo. Puedes tener hacking político, como un grupo ambientalista radical o un país.

P. En el caso de un minorista que recibe una infección de software de rescate (ransomware). ¿Qué medidas deben tomar?

R. Con suerte, estarían un poco preparados para un ataque de este tipo. El software de rescate ataca a la persona que ha hecho clic en el enlace equivocado. Puede suceder, y sucederá. Casi todas las empresas han sufrido este tipo de ataque. Un ordenador infectado no es un problema. Si el virus se puede propagar en la red interna, y no hay segregación, sus colegas probablemente se verán

afectados. Si es posible, la empresa debería haber segregado sus redes y parcheado sus sistemas. Es una buena idea ponerse en contacto con una empresa de seguridad. Sepa quién puede ayudarle. Como individuo, lo que puede hacer en caso de rescate (encriptación de un dispositivo) es que si nota que algo está siendo encriptado, apague la computadora. Pero definitivamente necesitarás la ayuda de expertos.

P. Las gasolineras del futuro se ven como estaciones de movilidad que incluirán una amplia gama de servicios, incluyendo servicios de entrega con drones, vehículos autónomos, compartir bicicletas... Todos estos servicios estarán fuertemente conectados y harán que el reto sea mayor.

R. El desafío será ciertamente más grande a medida que la exposición aumente. Aquí es donde entra la responsabilidad de los proveedores. Comprar componentes baratos de lejos que se producen en masa podría llevar a que millones de dispositivos de IO se vean comprometidos debido a una vulnerabilidad de seguridad. Lo barato puede conllevar muchos riesgos. Los proveedores tienen que asegurarse de que tienen un ciclo de actualización, auditorías de seguridad, tiempo de reacción rápida a las vulnerabilidades reportadas... Los fabricantes de esos componentes también son responsables de separar los componentes entre sí. Ahora debería ser posible activar los frenos de un coche infiltrándose en su sistema de medios. Debería haber una clara e incluso física segregación entre esos componentes. Sólo deberíamos permitir las conexiones que son realmente necesarias.

Entrevista de Oscar Smith Diamante

