Cómo se prepara la industria de servicios financieros para evitar y responder a los ataques cibernéticos sistémicos

10 de enero de 2019 | Por Gary B. Meshell (https://securityintelligence.com/author/gary-meshell/)

Thinkstock (http://www.thinkstockphotos.com/image/stock-illustration-bank-building-isolated-on-white/900791430)

Recientemente, antes de un importante día festivo en los EE. UU., Los ciberdelincuentes se dirigieron a varias compañías de pago y de tarjetas de crédito. Estas compañías recibieron la notificación de que si cada una no pagaba un rescate en bitcoin, se lanzaría un ataque cibernético contra la industria de pagos en el feriado, que es un día importante de compras. Los jugadores de servicios financieros y la aplicación de la ley pronto se concentraron para responder a este ataque cibernético sistémico en la industria.

En la industria de servicios financieros, una violación de datos es un problema de todos

Hasta hace poco, las empresas de servicios financieros se centraban casi por completo en la prevención de violaciones de datos que afectarían a sus propias organizaciones. Trataron de detectar riesgos de seguridad, como correos electrónicos de phishing, malware, bases de datos robadas y acceso remoto a redes, y detenerlos antes del auge, en el momento en que se descubre un ataque cibernético. Pero cada vez más, los servicios financieros y otras industrias están comenzando a reconocer que no se trata de si serán violados, sino cuándo. A la luz de esta realización, los esfuerzos del sector deben cambiar a la respuesta, no simplemente a la detección y prevención, y reconocer que estos ataques corren el riesgo de volverse de naturaleza sistémica, lo que afecta a toda la industria de servicios financieros.

Dada la interconexión que se ha desarrollado dentro de los servicios financieros, ninguna compañía puede operar en un vacío, ni para prevenir un ataque ni para responder a uno. Si hay una infracción dentro de un banco, por ejemplo, ese incidente pronto se extenderá a las redes de cajeros automáticos, proveedores de pagos, entidades de compensación y liquidación y servicios de terceros. La industria de servicios financieros se está preparando para la posibilidad de un ataque cibernético sistémico y se une en un esfuerzo por crear runbooks que definan los parámetros de una respuesta coordinada.

Líderes de la industria ponen a prueba su respuesta a incidentes

Este cambio ha llevado a los competidores a colaborar por el bien de la industria de servicios financieros. En octubre de 2018, por ejemplo, las compañías del Grupo de trabajo cibernético P20 y la Junta (https://www.youtube.com/watch?v=0Z2-nKOQ-O0) visitaron el X-Force Command Cyber Range de IBM (https://www.ibm.com/security/services/managed-security-services/security-operations-centers?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US) en Cambridge, Massachusetts, para un ejercicio de "juego de guerra". La industria global de pagos electrónicos, junto con representantes de la ley y del Departamento del Tesoro de los Estados Unidos, se unieron para un desafío de respuesta a ataques cibernéticos basado en el escenario vacacional mencionado anteriormente. La preparación para amenazas cibernéticas tradicionales se centra en evaluar los controles de tecnología y la integridad de los planes de respuesta a incidentes. Sin embargo, un ejercicio de juego de guerra cibernética (https://securityintelligence.com/cyber-war-games-top-payment-companies-collaborate-to-respond-to-financial-cyberattacks/) ofrece una oportunidad para modelar ataques y practicar la respuesta y la capacidad de recuperación en un entorno controlado.

El objetivo de la primera fase del ejercicio fue probar las comunicaciones de respuesta a incidentes, la efectividad de la toma de decisiones y la notificación a las partes interesadas durante una violación de datos. Esto resultó en un análisis de fortalezas, debilidades, oportunidades y amenazas (FODA) que mostró más debilidades que fortalezas.

En el lado positivo, hubo una buena coordinación organizativa entre el liderazgo y los equipos multifuncionales. Dicho esto, quedó claro que la industria todavía carece de una taxonomía común en torno a la gestión de crisis, incluido lo que incluso constituye una crisis. No se establecieron procesos ni enlaces para involucrar al gobierno o la aplicación de la ley. La mayoría de los directores de seguridad de la información (CISO) carecían de capacitación en medios, y por lo tanto no sabían con quién comunicarse o qué comunicar en las declaraciones de los medios (https://securityintelligence.com/media/get-smarter-about-disaster-response-five-resolutions-for-2018/) . Los desafíos abundaban en detección, investigación y respuesta. Finalmente, no hubo intención del comandante de dirigir cómo se vería un resultado exitoso.

La intención del comandante es crucial para un plan de respuesta sistémica

De muchas maneras, un ataque cibernético es similar a un ataque militar, según el teniente coronel Hise Gibson, un profesor visitante de la Escuela de Negocios de Harvard. Gibson se especializa en aplicar las lecciones aprendidas en el campo de batalla a los ataques cibernéticos en el mundo de los negocios. Cuando el comando está descentralizado, ya sea en coaliciones militares o empresas de servicios financieros, la creación de equipos cohesivos depende de la confianza mutua.

El equipo debe crear un entendimiento compartido que resulte en una clara intención del comandante, o una "descripción y definición de cómo será una misión exitosa", según Harvard Business Review (https://hbr.org/2010/11/dont-play-golf-in-a-football-g) . En un contexto empresarial, la intención del CEO empodera a los subordinados y guía la iniciativa y la improvisación en caso de un evento caótico, como una crisis cibernética.

La fase dos del ejercicio del juego de guerra consistió en crear una simulación de respuesta a incidentes personalizada y de alta fidelidad para la industria de servicios financieros. La simulación permitió a los participantes trabajar juntos para desarrollar un libro de jugadas iterativo para responder a incidentes, lo que requiere un marco para la colaboración entre compañeros y compañeros y el intercambio de datos.

Aprende más

Entrena con el primer equipo cibernético de fuerzas especiales del mundo (https://www.ibm.com/security/services/managed-security-services/security-operations-centers?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US)

3 lecciones que informan a la próxima generación del rango cibernético (https://securityintelligence.com/3-lessons-that-are-informing-the-next-generation-of-the-cyber-range/)

Un plan de respuesta consistente de “romper el cristal” depende de que los individuos tengan la capacidad de actuar. En lugar de pedir fondos, el líder debe poder gastar lo que necesita; En lugar de preocuparse por pisar los dedos de los pies, él o ella debe tener la capacidad de hacer que los clientes estén completos. Mientras tanto, el equipo debe practicar el plan de respuesta hasta que se vuelva tan natural como la memoria muscular.

Crear un flujo de trabajo que habilite la orquestación de respuesta a incidentes

En la fase tres del ejercicio, los participantes de la industria de servicios financieros crearán un flujo de trabajo que detalla la respuesta a un ataque cibernético sistémico. La orquestación inteligente (https://www.ibm.com/security/intelligent-orchestration?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US) apoyará una respuesta guiada a ataques complejos con libros de jugabilidad ágiles que pueden adaptarse a los detalles del incidente en tiempo real y establecer roles, responsabilidades y plazos. Esta preparación en última instancia permitirá a las empresas de servicios financieros contener efectivamente los incidentes y evitar un efecto dominó que derribe a la industria.

Las empresas de servicios financieros deben continuar colaborando con sus pares de la industria, crear ejercicios de respuesta de la industria y runbooks, y probar rigurosamente sus planes en instalaciones como el Centro de Comando de IBM X-Force. Obtenga más información sobre el X-Force Command Center de IBM (https://www.ibm.com/security/services/managed-security-services/security-operations-centers?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US) y cómo las compañías están trabajando para prepararse para su peor día.

Etiquetas: Seguridad bancaria (https://securityintelligence.com/tag/bank-security/) | Ciberataques (https://securityintelligence.com/tag/cyberattacks/) | Industria financiera (https://securityintelligence.com/tag/financial-industry/) | Instituciones financieras (https://securityintelligence.com/tag/financial-institutions/) | IBM X-Force Command Center (https://securityintelligence.com/tag/ibm-x-force-command-center/) | Respuesta a Incidentes (IR) (https://securityintelligence.com/tag/incident-response-ir/) | Respuesta de amenaza (https://securityintelligence.com/tag/threat-response/) | X-Force (https://securityintelligence.com/tag/x-force-2/)


https://securit
-hell/)

Gary b. Meshell (https://securityintelligence.com/author/gary-meshell/)
Líder mundial de ventas y desarrollo de negocios, IBM
Gary B. Meshell es un reconocido líder en temas de seguridad y nube dentro de los servicios financieros ...
4 mensajes (https://securityintelligence.com/author/gary-meshell/)

Comparte este artículo:

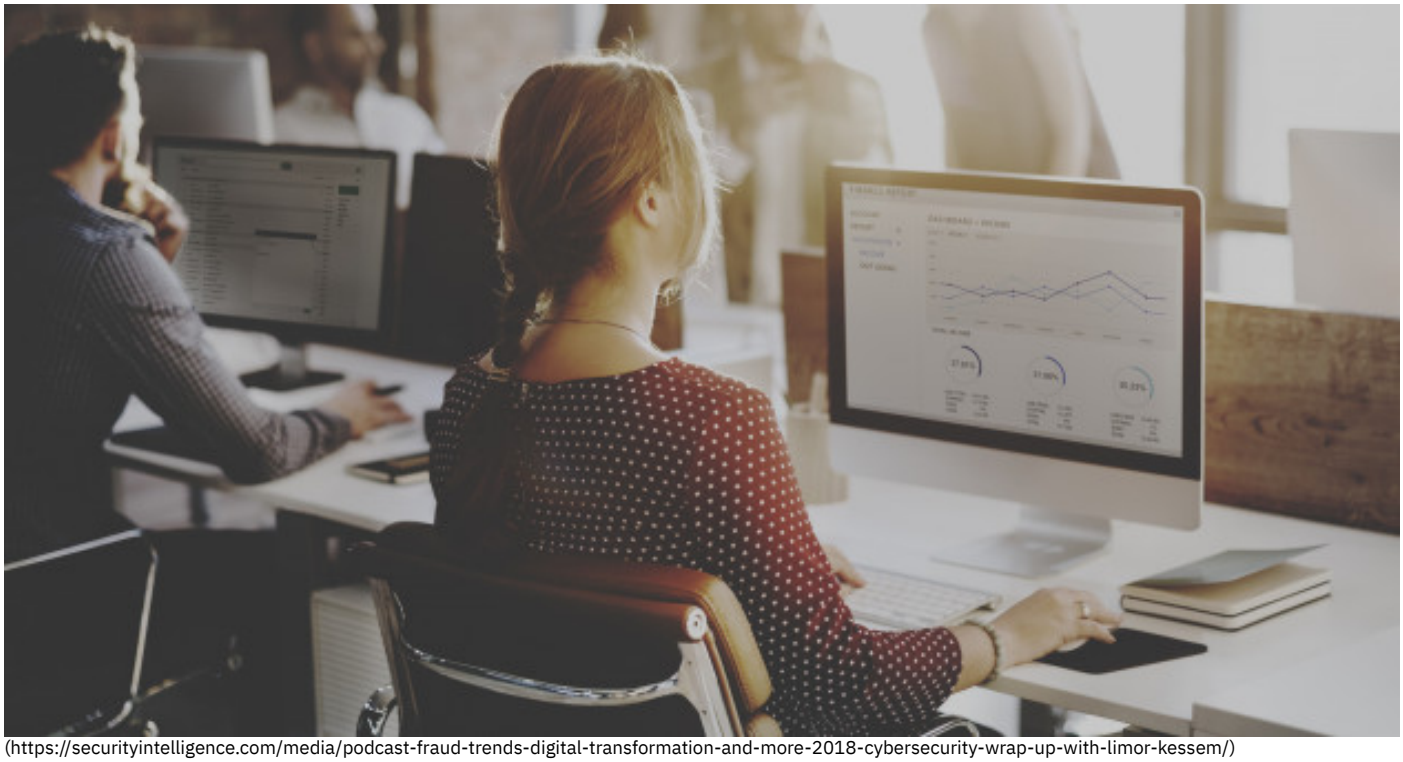
(https://twitter.com/intent/tweet?url=https%3A%2F%2Fsecurityintelligence.com%2Fhow-the-financial-services-industry-is-preparing-to-avoid-and-respond-to-systemic-cyberattacks%2F)

More on Banking & Financial Services

(https://securityintelligence.com/media/podcast-digital-identity-trust-part-3-powering-digital-growth-with-digital-identity-trust/)

Podcast

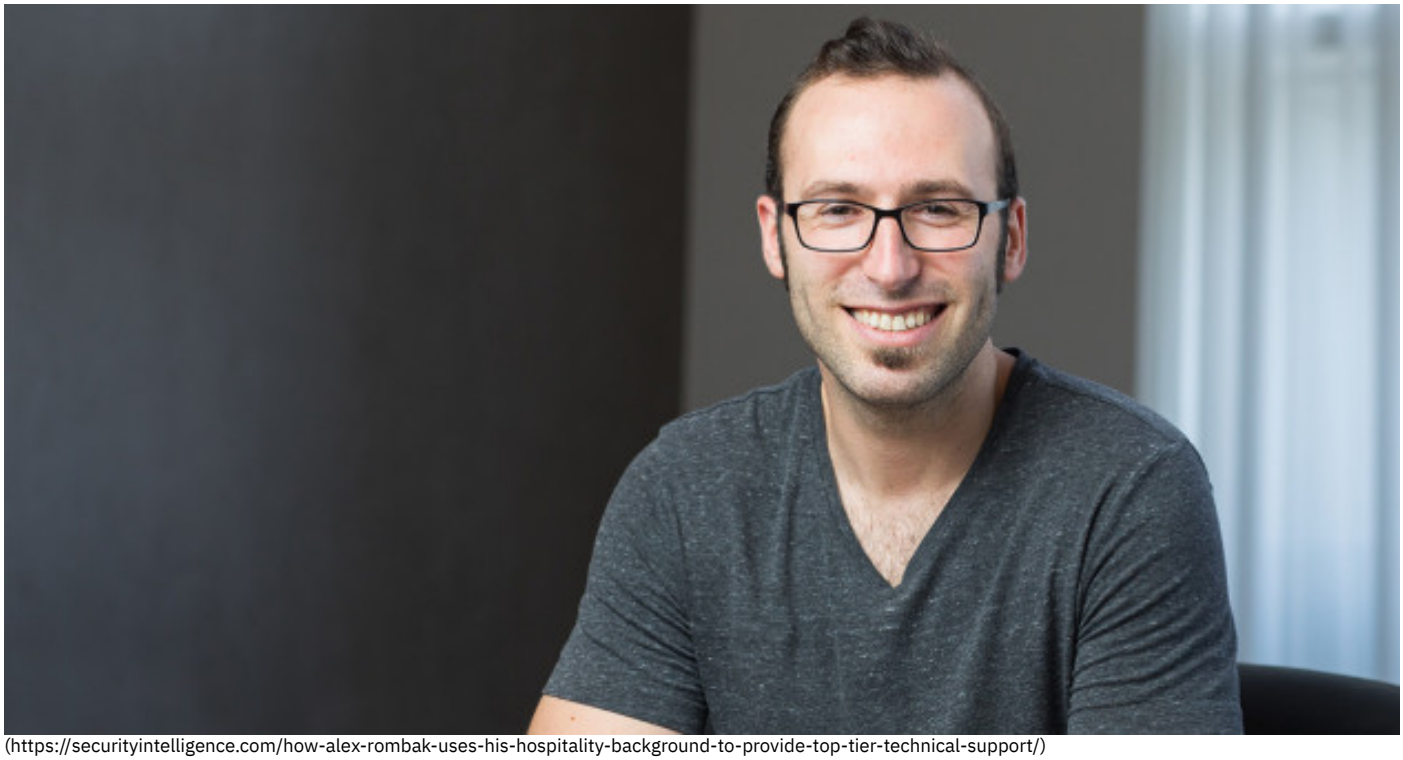
Podcast: Digital Identity Trust, Part 3 — Powering Digital Growth With Digital Identity Trust (https://securityintelligence.com/media/podcast-digital-identity-trust-part-3-powering-digital-growth-with-digital-identity-trust/)



(https://securityintelligence.com/media/podcast-fraud-trends-digital-transformation-and-more-2018-cybersecurity-wrap-up-with-limor-kessem/)

Podcast

Podcast: Fraud Trends, Digital Transformation and More — 2018 Cybersecurity Wrap-Up With Limor Kessem (https://securityintelligence.com/media/podcast-fraud-trends-digital-transformation-and-more-2018-cybersecurity-wrap-up-with-limor-kessem/)



(https://securityintelligence.com/how-alex-rombak-uses-his-hospitality-background-to-provide-top-tier-technical-support/)

Article

How Alex Rombak Uses His Hospitality Background to Provide Top-Tier Technical Support (https://securityintelligence.com/how-alex-rombak-uses-his-hospitality-background-to-provide-top-tier-technical-support/)

(https://securityintelligence.com/continuous-compliance-eases-cloud-adoption-for-financial-services-firms/)

Article

Continuous Compliance Eases Cloud Adoption for Financial Services Firms (https://securityintelligence.com/continuous-compliance-eases-cloud-adoption-for-financial-services-firms/)

(https://securityintelligence.com)