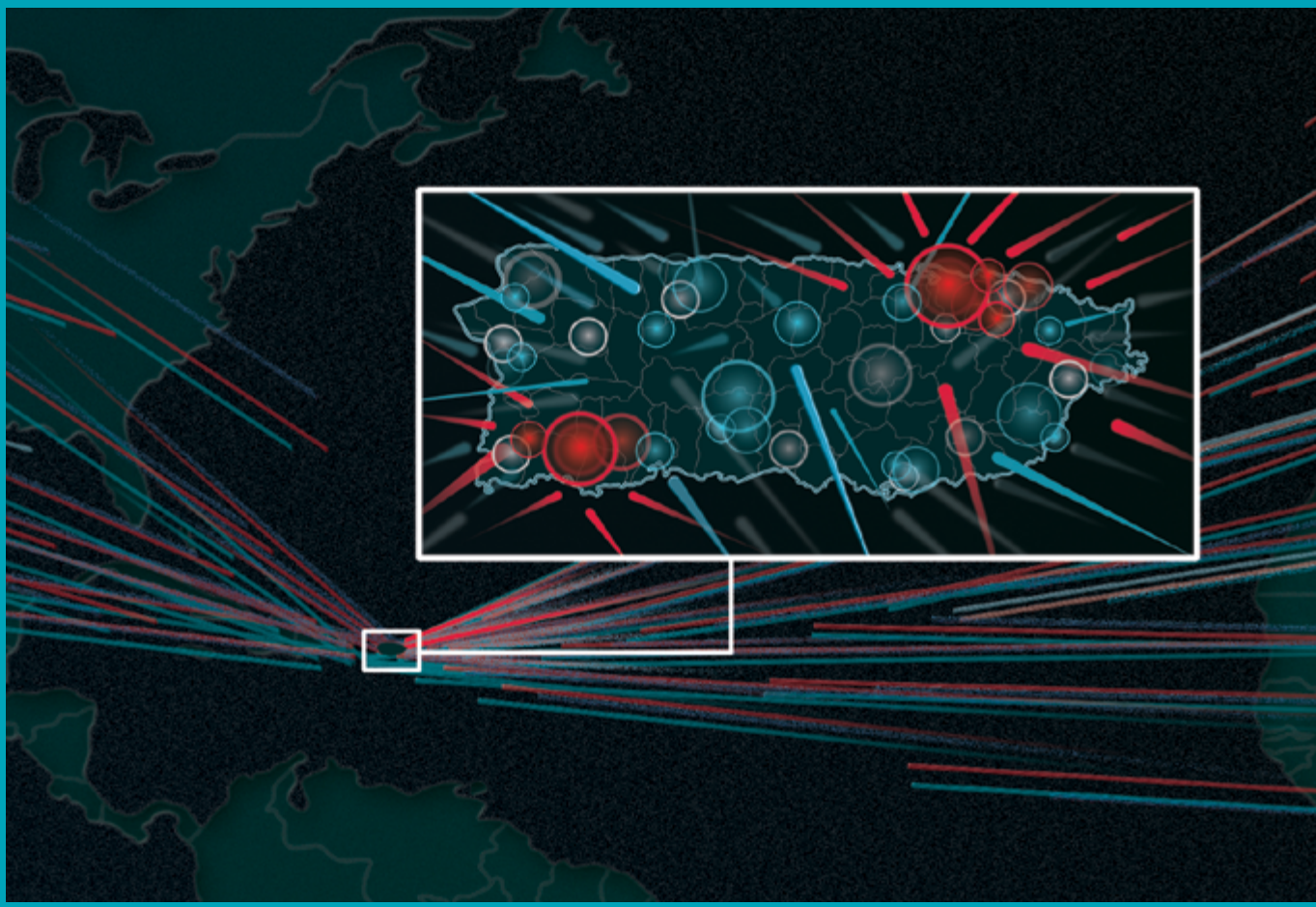
ESTUDIO DE CASO
RANSOMWARE
HACIENDA DE PUERTO RICO

Teléfono: 443-345-0503
infopr@compsecdirect.com
www.compsecdirect.com



Fecha de publicación:
21 de junio, 2021
Illustración: María de los Ángeles Pagán

 TODOS LOS DERECHOS RESERVADOS

José Fernández
Presidente

GRACIAS
POR LEER ESTE ESTUDIO

Puerto Rico enfrenta varias dificultades que aparentan ser imposibles de arreglar. Como puertorriqueño, es necesario reconocer los esfuerzos que colectivamente efectuamos para tratar de mejorar la calidad de vida de sus ciudadanos. No obstante, necesitamos aprender de errores pasados. No para humillar ni denigrar, si no para entender cómo se puede prevenir situaciones similares en el futuro cercano. Hacienda pudo haber sido hackeado en el 2017, muchas empresas se ven expuestas de la misma manera. Somos optimistas de que las cosas van a mejorar y entendemos que este estudio ofrece una solución.

151 Calle San Francisco
Suite 201
San Juan, PR, 00901

Teléfono: 443-345-0503
E-mail: infopr@compsecdirect.com
www.compsecdirect.com

Contenido: José Fernández
Diseño: María de los Ángeles-Pagán
Mercadeo y prensa: Ivette Rodriguez
Revisiones: Oscar Fuentes

 TODOS LOS DERECHOS RESERVADOS

CONTENIDO

02 Introducción / Hechos básicos

04 Resumen ejecutivo

05 Hechos condensados

06 Defensas proactivas

08 Resumen de eventos

10 Eventos históricos

11 Perfil de actacante / Retos informáticos

12 Ámbito de acciones

13 Salida del evento / Recomendaciones estratégicas

14 Conclusiones

15 Recomendaciones

Agradecimientos: Heriberto Acosta, Giancarlo Gonzales Ascar, Fortaleza de Puerto Rico, Hacienda de Puerto Rico, BSides PR.

EL RAYO CAE DOS VECES Y LOS

CIBERNÉTICOS NUNCA DUERMEN

CompSec Direct proveyó los esfuerzos iniciales de respuesta para el Departamento de Hacienda de Puerto Rico durante un ataque cibernético.

Nuestro estudio de caso destaca como liderazgo efectivo, coordinación de acciones y medidas preventivas pueden prevenir situaciones similares con las que se enfrentó Hacienda. El presidente de CompSec Direct estuvo presente en reuniones de estrategia con altos funcionarios dentro del Departamento de Hacienda, reuniones con ejecutivos y funcionarios del Negociado de Investigaciones Federales.

Información técnica, como registros de seguridad digital, imágenes de datos binarios relacionados a ransomware, diagramas de redes y entregables de grupos terceros fueron compartidos con nosotros y formulan parte de nuestro asesoramiento de este estudio.

CompSec Direct proveyó la orientación, recomendaciones y listas de acciones para que Hacienda siguiera durante un ataque de ransonware en el 2017.

HECHOS BÁSICOS

... PARA AQUELLOS QUE NO CONOCEN A HACIENDA.

La organización tiene déficit de personal

Hacienda depende en contratistas que están abrumados con tareas y simplemente no pueden mitigar efectivamente fallas tecnológicas en su ámbito.

Las metas de seguridad de IT no están definidas

Aunque es difícil implementar una estrategia efectiva para "defender todo y a todas horas" en una organización complicada con varios sistemas; esta organización recauda ingresos para la isla y no es capaz de prevenir riesgo digital innecesario.

Funcionarios del gobierno son responsables

Equipo de IT no contaba con buen equipo, organización, ni adiestramiento para manejar una situación de ransomware. Conocimiento de fallas existentes de seguridad y debilidades tecnológicas de los sistemas es responsabilidad de empleados gubernamentales, los cuales dependen en contratistas para informar y atender estas fallas de manera transparente y con exactitud.

Esfuerzos de restauración de servicios demostró vacíos de liderazgo.

La organización no contaba con un ejecutivo de seguridad de informática o CISO al transcurrir el ransomware. Tener este puesto vacante es el resultado del éxodo de talento que existe en la isla. La escasez de experiencia en nuestro talento local contribuye a la laguna de puestos ejecutivos con cargos de responsabilidad. El periodo de transición entre administraciones gubernamentales empeora este vacío.

TODOS LOS DERECHOS RESERVADOS

Síguenos en LinkedIn: compsec-direct y en Facebook CompSecDirect

RESUMEN EJECUTIVO

HECHOS BÁSICOS

En el 5 de marzo del 2017, el Departamento de Hacienda reporta que sus sistemas digitalizados sufren de averías parciales de servicios a los medios:

> **Fuentes de ingreso estatal quedan impactadas**

> **La Autoridad de Puertos es incapaz de cobrar impuestos en todo comercio marítimo.**

> **Compañías y residentes de la isla no pueden rendir informes relacionados a pagos de IVU**

Hacienda destaca sus perdidas en exceso de $20 millones de dólares diarios debido a su avería

El Departamento de Hacienda (DOH) considera que los sistemas impactados empiezan durante un periodo reservado para hacer actualizaciones de sistemas. Luego establece ser víctima de Ransomware.

Enlace del 6 marzo, 2017 artículo de El Nuevo Dia publicado: ElNuevoDia.com

RESUMEN EJECUTIVO
HECHOS CONDENSADOS

Equipo de IT identifica el Ransomware

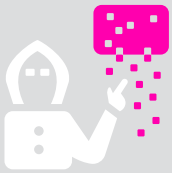
Integrantes del equipo de IT de Hacienda (EITH) determinaron que Ransomware se propago entre servidores y estaciones de trabajos dentro de su red informática. Los daños ocasionados a sus sistemas son extensos y se solicita ayuda de expertos para remediar la infección.

Enfoque de restauración

CompSec Direct y otros fueron contactados para ayudar al DOH con sus esfuerzos de restauración de operaciones. El gobierno correctamente solicito ayuda de expertos en seguridad de informática que residen en la isla.

Trabajo se dividió entre tres equipos

Expertos lograron proveer dirección para el DOH en las primeras 48 horas de la infección, permitiendo que el DOH continuara recaudando fondos gracias a los esfuerzos del gobierno de Puerto Rico, el EITH y CompSec Direct.



La confianza interna esta fragmentada

Conflictos de contratos ocurrieron meses antes del ransomware. Auditores expresan falta de integridad y protección de sus comunicaciones internas por parte del EITH.

El FBI ejecutó arrestos relacionados a crímenes

No existe evidencia pública que apoye una teoría que vincule el crimen interno de Hacienda con el ataque de ransomware del 2017. Los acusados merecen el beneficio de duda hasta que se concluyan las investigaciones y los procedimientos legales.

Nosotros proveímos asesoría estratégica

CompSec Direct proveyó el plan inicial de respuesta ante el ataque ransomware de Hacienda del 2017. Ayudamos a coordinar y mitigar los efectos del ransomware en las operaciones de esta organización.

Enlace del 7 marzo, 2017 artículo de El Nuevo Dia publicado: Gloria Ruiz Kuilan @ ElNuevoDia.com

ESTO PUDO HABER

SIDO EVITADO

Defensas-proactivas

Escaneo, monitoreo, y pruebas digitales de su infraestructura antes de que ocurran problemas

Requiere validación independiente por un grupo externo

Validación externa

Usando un sistema de escaneo interno ayuda a los dueños de sistemas a entender su ecosistema. Usando escaneo externo se demuestra como el ecosistema es accesible de manera remota.

Vigilancia digital

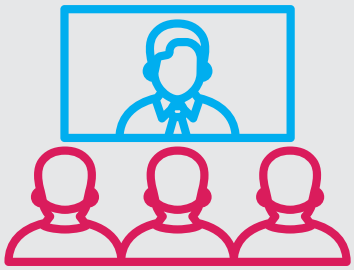
El ecosistema digital sobrepasa el número de empleados. Sin un sistema entallado a medida, sus empleados y contratistas no podrán responder efectivamente a incidentes digitales.

Pruebas digitales

Pruebas de fallas y recuperación de operaciones deber ser recurrente. El proceso mide como los objetivos de recuperación se logran bajo situaciones previstas antes de ocurrir. El refinamiento mejora vacíos a través de la repetición. Personal interno ya se encuentra enfocado en mantener operaciones, no en hacer sus operaciones más fuertes y resistentes.

 TODOS LOS DERECHOS RESERVADOS

NUESTRAS ÁREAS DE ESPECIALIZACIÓN APLICABLES A LOS SUCESOS



Adiestramiento personal

Queremos ayudar a sus empleados progresar, sin reemplazar a sus empleados existentes. Nuestros expertos asesoran y adiestran a sus empleados para colectivamente mejorar su capacidad de visualizar y entender cómo responder a nuevas amenazas digitales desconocidas.

Protección de ransomware

Prevenir incidentes es más económico que remediar un evento a la misma escala que el que sufrió Hacienda en el 2017. Ransomware no se puede prevenir con una sola herramienta. CompSec Direct puede ayudar a su equipo en identificación y manejo de riesgo antes que sea muy tarde.

DESEAMOS QUE SE COMUNIQUE CON NOSOTROS PARA MÁS INFORMACIÓN DE ESTOS SERVICIOS

Caza digital como servicio

CompSec Direct puede defender su empresa de manera presencial o remota, para cazar amenazas en sus redes. Este servicio requiere tiempo para maximizar su inversión mientras se facilita el monitoreo digital y sus recursos humanos.

Respuesta a incidentes digitales

El tiempo es crítico durante una brecha. Se requiere que la organización se comunique con expertos para reducir el impacto de un incidente digital negativo tal como ransomware. Poseer acuerdos preestablecidos reduce el tiempo dedicado a negociación y permite que los expertos se enfoquen en el problema; su brecha actual y no su proceso de adquisición.

TODOS LOS DERECHOS RESERVADOS

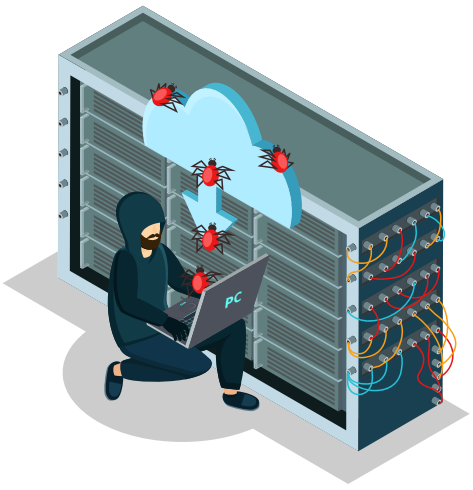
Síguenos en LinkedIn: compsec-direct y en Facebook CompSecDirect

RESUMEN DE EVENTOS

EJECUCIÓN DE ESTRATEGIA AGILIZADA

- **COORDINACIÓN ENTRE GRUPOS NO FUE EFECTIVA NI CONSOLIDADA EN UNIÓN**
- **EJECUTIVOS DE HACIENDA RELACIONAN UNA INVESTIGACIÓN DE CRIMEN INTERNO COMO MOTIVACIÓN PARA EL ATAQUE DE RANSOMWARE.**
- **EL GOBIERNO DE PUERTO RICO INFORMA DE HABER ABANDONADO SU TEORÍA DE CRIMEN INTERNO DENTRO DE HACIENDA COMO MOTIVACIÓN PARA EL RANSOMWARE Y AHORA CULPA A CHINA POR LOS SUCESOS.**

CompSec Direct proveyó planes de acción para integrantes del equipo del sistema Windows® y el equipo de redes para utilizar durante el incidente de ransomware.



El FBI arresta a dos empleados de Hacienda por corrupción

"Los hombres están acusados de extorsión y soborno."

Enlace del 9 marzo, 2017 artículo de El Nuevo Dia publicado: Frances Rosario @ ElNuevoDia.com

BRECHA DE DATOS, RANSOMWARE,

Resumen de eventos del 7 de marzo al 9 de marzo 2017

- EL JEFE DE INFORMÁTICA (CIO) DE PUERTO RICO SOLICITÓ UN PLAN DE COORDINACIÓN INMEDIATO ENTRE TRES EQUIPOS:

> Respuesta de incidentes (IR): CompSec Direct
> Monitoreo interno: Equipo de IT de Hacienda (EITH)
> Análisis de malware: 6th Element Group, ahora FiberWolf

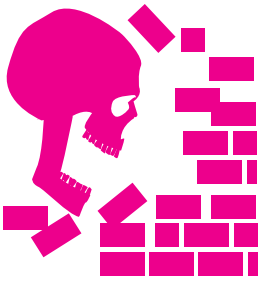
- COMPSEC DIRECT IDENTIFICA QUE DOS INTEGRANTES DEL EITH SON RESPONSABLES POR LA SEGURIDAD DE INFORMÁTICA DE HACIENDA; UNA ORGANIZACIÓN CON MÁS DE 5000 USUARIOS DE SISTEMAS.

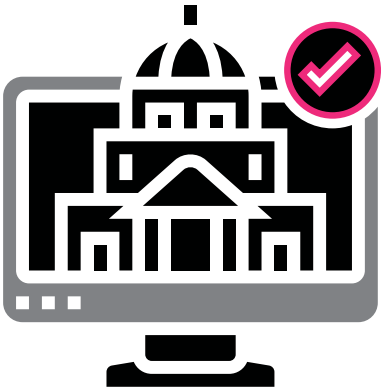
- EJECUTIVOS DE HACIENDA EN EL 2017 CREEN QUE AGENTES DEL FBI PUEDEN AYUDAR RESOLVER SU PROBLEMA DE BRECHA DE SISTEMAS, DURANTE Y DESPUÉS DE SU CRISIS DE RANSOMWARE.

- UN INTEGRANTE DE ASUNTOS INTERNOS DE HACIENDA EXPRESA SOSPECHAS QUE INTEGRANTES DEL EITH LEEN COMUNICACIONES SENSITIVAS SOBRE SOBORNOS Y EXPEDICIÓN ILEGAL DE PERMISOS.

¿COMO SUCEDIÓ ESTO?

EVENTOS HISTÓRICOS ANTES DE BRECHA POR RANSOMWARE

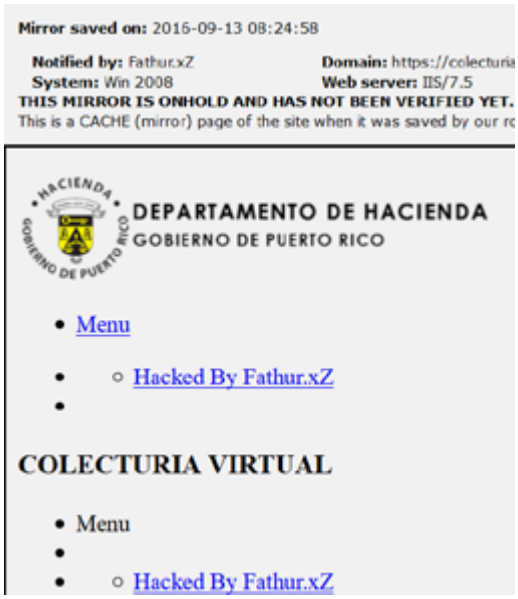




El gobierno de Puerto Rico tiene antecedentes históricos en fallas de seguridad dentro de sus sistemas digitalizados.

No obstante, Puerto Rico ha logrado proveer valor en sus esfuerzos para brindar servicios digitales a sus residentes y comerciantes como parte de su estrategia de digitalización de servicios gubernamentales.

Hacienda y otros funcionarios públicos minimizaron el impacto de una brecha anterior en 2016, citando que no hubo hurto de archivos digitales, aunque claramente fueron haqueados.



Hacienda se encontraba en un periodo de conflicto con sus contratistas, por razones desconocidas, los cuales son proveedores establecidos de servicios de IT en Puerto Rico. Estos conflictos quizás han resultado en bajas de posiciones mientras el gobierno anuncia declararse en quiebra en un periodo continuo de inestabilidad económica.

Hacienda confirma su brecha de 2016, evidente en su pagina de colecturía.

La desfiguración de su página fue ejecutada por un hacker llamado **Fathur.xZ**.

Este apodo de hacker está afiliado con el equipo de Libertad Ciber de Indonesia (Indonesian Cyber Freedom o INCEF).

PERFIL DE ATACANTE: FATHUR.XZ

Cuentas de Twitter:
fathur Xz'aliDce-AOH
@fathurAOH

Sobre 2,900 páginas jaqueadas segun Zona-H.

Integrante conocido del equipo Libertad Ciber de Indonesia

Alta confianza en atribución.

Hizo/vendió camisas en **TeeSpring**

Diseño hecho por Fathur.xZ con el logo del dragón de Kali Linux
Alta confianza en atribución.

Análisis de brecha:

Hacienda presuntamente facilitó la brecha del 2016 al dejar activo acceso al instalador del portal de manejo de contenido (CMS) que usa.

La brecha del 2016 **no aparenta** ser dirigida explícitamente contra Hacienda.

TEESPRING PUEDE PROVEER LOS REGISTROS DE ACCESO A LA CUENTA QUE EL INDIVIDUO PRESUNTAMENTE USA PARA MANEJAR VENTAS EN ESE PORTAL PARA AYUDAR ATRIBUIR SU IDENTIDAD VERÍDICA.

DIFICULTADES DE IT QUE IMPIDEN QUE HACIENDA PREVENGA RANSOMWARE Y DISMINUCIÓN DE LA EFECTIVIDAD DE CIBER-SEGURIDAD

01
Conflictos de contratos
Allegadamente y a pesar de altos niveles de desempleo, Hacienda depende en exceso en contratistas.

02
Ningún CISO
No existe un ejecutivo que pueda comunicar riesgos de IT expresados por empleados y contratistas en Hacienda.

03
Deuda técnica
Sistemas variados, modernos y antiguos, que hacen crecer gastos de operaciones bajo sustento é impide cambios dirigidos a reducir riesgos.

04
Escasez de controles y monitoreo de fronteras digitales
Hacienda fue jaqueado en el 2017 por no reducir su superficie de ataque externa.

05
Falta de operaciones de seguridad
No existe un equipo, independiente de IT, dedicado a caza de amenazas digitales ni un equipo forense digital dedicado a respuesta de incidentes. Un SOC externo no es adecuado para esta organización debido al punto #1. Hacienda tendrá dificultad en aceptar recomendaciones de prevención y remediación debido a coincidencia de contratistas y sus contratos existentes.

TODOS LOS DERECHOS RESERVADOS

Síguenos en LinkedIn: compsec-direct y en Facebook CompSecDirect

ÁMBITO DE ACCIONES

Hallazgos claves y recomendaciones

- Es más útil desconectar equipo afectado de la red usando reglas de acceso y/o desconexión física. Esto ayuda a preservar evidencia dinámica del sistema en equipo virtual en la nube y equipo físico, en vez de apagar equipos afectados.

Equipo de IT debe de continuar cumpliendo sus responsabilidades normales en vez de convertirse en analistas de forense digital

- Es difícil convencer al equipo de IT en seguir sus funciones normales al sentirse responsables de brechas. Intentarán arreglar problemas sin adiestramiento. Al estar bajo presión, cometerán errores adicionales sin planificar las remediaciones necesarias.
- Denegamos entrevistas de prensa ya que el incidente no estaba contenido en ese momento. Se le informa a Hacienda y a Fortaleza que entrevistas provocan a los agresores, y quizás su brecha pudo haber sido peor.

EFECTOS DE NUESTRO INVOLUCRAMIENTO EN EL PRIMER DÍA

- **CompSec Direct ayudo Hacienda a resumir generación de ingresos para Puerto Rico.**
- Nosotros ayudamos a dirigir las primeras acciones de respuesta encaminadas a respaldo y recuperación de datos en sus respectivos sistemas.

ESTRATEGIA DE RESPALDO Y REFUERZO DIGITAL

DÍA 2

- Informa el EITH que ataques adicionales mediante variantes del ransomware fueron ejecutados dentro de la red.
- Proveímos listas de tareas y acciones para los administradores de sistemas Windows® y administradores de firewalls. Las tareas estaban divididas por su propósito forense y defensivo.

"Sangre en el agua" ocurrió al observar cómo entran vendedores de compañas establecidas y ocupan tiempo dando presentaciones, sin tener especialización ni conocimiento en seguridad de informática, lo cual Hacienda necesitaba retroactivamente.

DÍA 2 ENTREGA DE PROPUESTA

CREACIÓN DE UN PLAN INMEDIATO

RESPUESTA COMPRENSIVA

Ejecutar respuesta de ransomware, fortalecer sistemas y red, recopilar documentación para ayudar procesos legales.

REDUCCIÓN DE GASTOS

Adquisición de programas necesarios para remediar problemas existentes; respetando la deuda y crisis económica actual.

LA MEJOR OFERTA

Los servicios proveídos por Microsoft no eran iguales a nuestra propuesta. Incluimos modificaciones de sistemas y defensas-proactivas en conjunto con nuestra propuesta.

SALIDA DEL EVENTO RANSOMWARE

NUESTRA RECOMENDACIÓN FINALIZACIÓN DEL DÍA 2

Recomendamos que Hacienda pagara un Bitcoin (aproximadamente $1,200 en marzo 2017) para recuperar un sistema que contenía sus respaldos actualizados de manera física. Esta recomendación era la manera más costo efectiva de recuperar su información luego de considerar todas las alternativas. Servicios de recuperación por desciframiento no son garantizados. Otra compañía intento comunicarse con los operadores de ransomware, sin logro.

> “Respuesta de incidentes es el equivalente de pagarle a alguien por la falta de preparación y visión de una organización. Nosotros entramos, removemos los problemas que identificamos, mantenemos visibilidad por un tiempo para asegurar que no olvidamos cotejar algo y no ofrecemos ninguna garantía de que la organización esta más segura por nuestros esfuerzos.” **Preparación, adiestramiento y contratación externa son los enemigos de incidentes.**

DISCUSIONES CON EL FBI

LA CARGA DEL DESCUBRIMIENTO DE PRUEBAS Y LAS EXPECTATIVAS HACIA LOS FEDERALES

DÍA-3

Hacienda piensa que el FBI arreglaría sus problemas

La escasez de profesionales en seguridad de informática a nivel federal ha creado demoras en procesar casos. Se informa a Hacienda que el FBI no asegura las redes de víctimas de crímenes digitales.

RECOMENDACIONES ESTRATÉGICAS

RESULTADOS SON POSIBLES, AUNQUE EXISTAN PROBLEMAS ECONÓMICOS

Usar internados de 6 a 12 meses para empleos

Reclutar aspirantes de seguridad de IT en ferias de empleos en universidades y en eventos enfocados como BSides PR.

Desarrollar y probar su proceso de recuperación de desastres

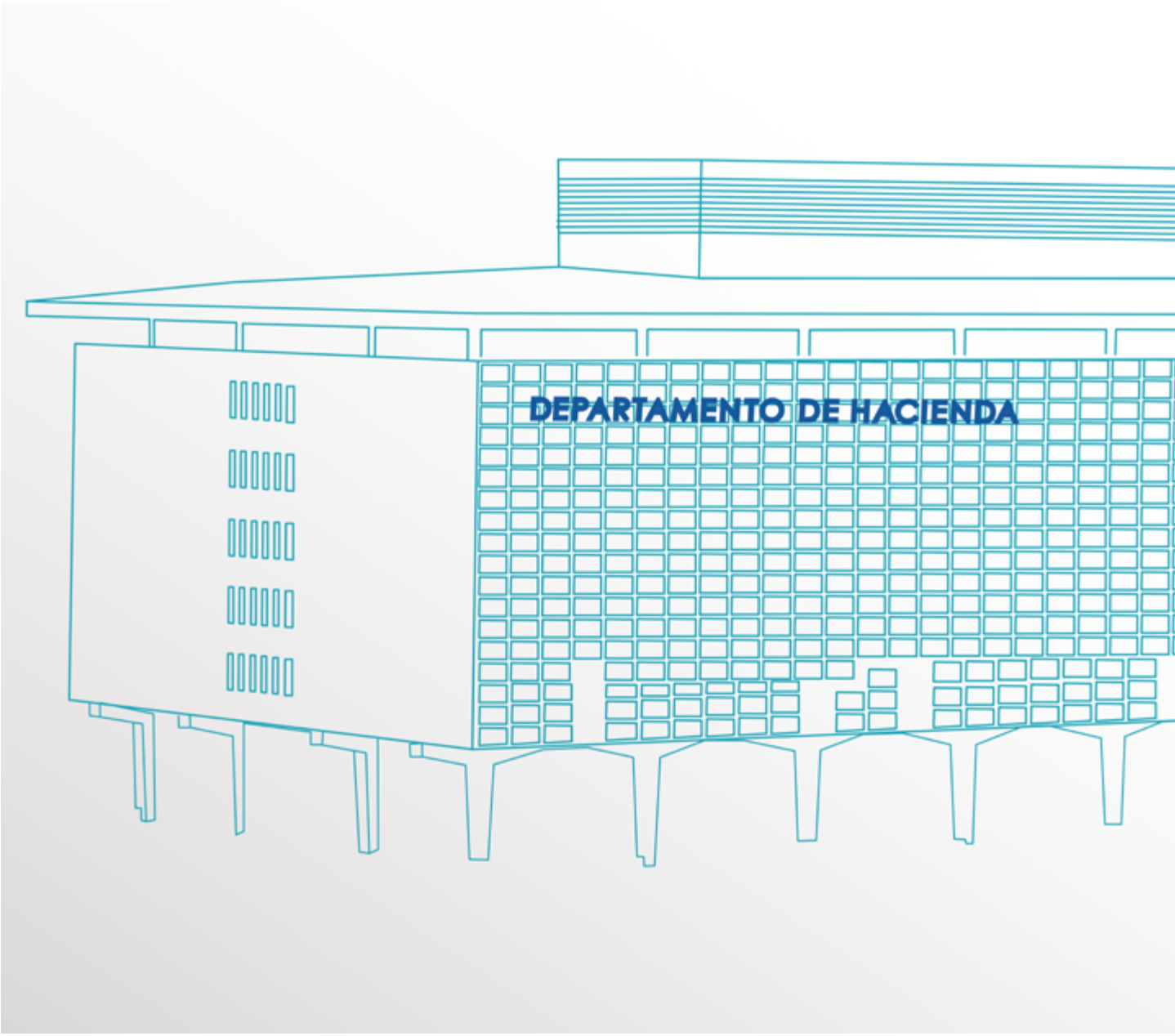
Probar distintas situaciones ante su efectividad del plan y las estrategias necesarias a fin de mejorar el tiempo requirido para recuperar cada sistema.

CompSec Direct informó al FBI y redujo el descubrimiento de hechos

Luego de atender una reunión pre-informe, nosotros ayudamos a estructurar las acciones que se habían tomado hasta ese día en relación con el evento de ransomware. Limitamos nuestras discusiones a hechos relevantes para poder ayudar en cualquier investigación futura.

Desarrollar y entrenar integrantes con más experiencia en Hacienda

Aumentar el adiestramiento del EITH en manejo adecuado de incidentes digitales, incluyendo medidas en relación con decisiones e informes necesarios para documentar eventos similares. Recomendamos que los contratistas existentes sean excluidos debido conflictos mencionados en este informe. Sin inversión en adiestramiento en integrantes veteranos de Hacienda, sus habilidades se estancan y quizás dejen sus plazas por otras oportunidades sin considerar continuidad de tareas ni compartir conocimiento operacional antes de separarse.



HACIENDA

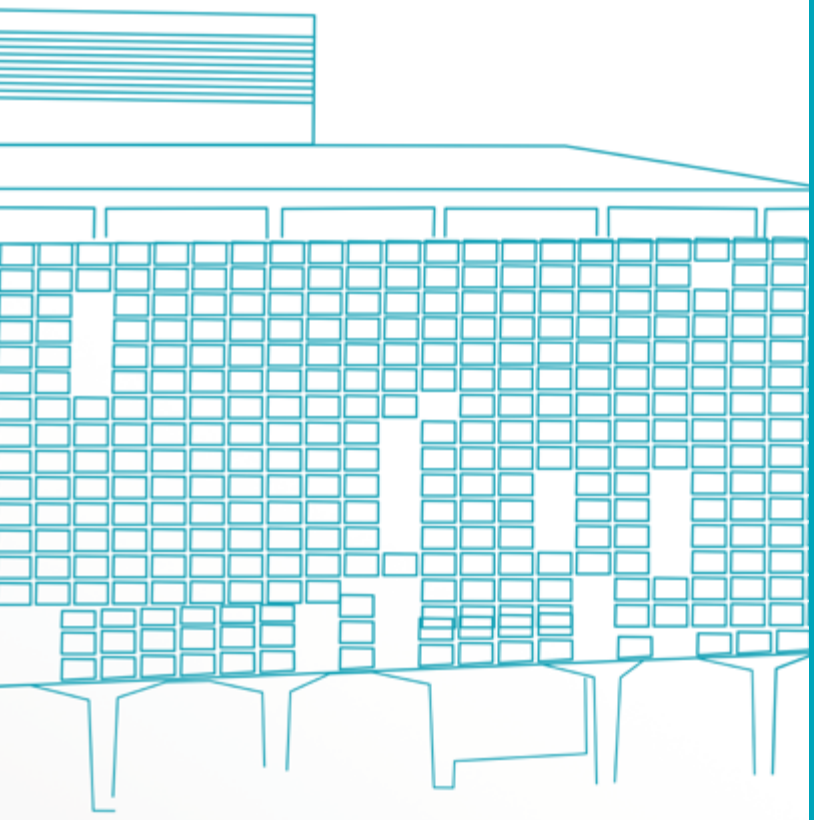
SALIDA

Conclusiones

Todas las señales y advertencias estaban presentes:

1. Brecha anterior
2. Controversias con contratistas de IT
3. Sospechas de usuarios abusando accesos y tramites ilícitos
4. Cambio de funcionarios por elecciones

- ☑ Los problemas que Hacienda enfrentó en 2017 quizás todavía existen.
- ☑ Todos somos Hacienda; ninguna organización es inmune a sabotaje por personas internas ni hackers organizados.
- ☑ Planificación de recuperación de desastres tiene que ser redundante debido al bajo costo de almacenaje.
- ☑ El "Cloud" no es un lugar ideal para un "Hot-Site" cuando los respaldos exceden de 1 Tb y sus "uplinks" no tienen velocidad.
- ☑ El gobierno de Puerto Rico requiere verdaderos expertos de proveedores especializados en seguridad para asistencia futura.



LE EXHORTAMOS QUE NOS CONTACTEN PARA ENTENDER SUS NECESIDADES Y APRENDER MÁS SOBRE NUESTRAS SOLUCIONES, ESTRATEGIAS Y PARA OPCIONES DE PRECIO DE NUESTROS SERVICIOS

www.compsecdirect.com
infopr@compsecdirect.com

(443) 345-0503

151 Suite 200, San Juan, PR 00901

Recomendaciones

Le aconsejamos a Hacienda en cuales sistemas podrían ser restaurados y ayudamos a Puerto Rico a generar millones de dólares debido a nuestras recomendaciones.

Coordinar con el FBI para determinar parrandero de carteras digitales asociadas con el ransomware.

Coordinar a través del FBI en identificar sistemas asociados a Tor que registraron y facilitaron pagos del como un crimen grave y serio.

CompSec Direct es una empresa con oficinas en Puerto Rico y Maryland dedicada a C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance). Somos una compañía certificada SDVOSB, socios con Amazon AWS, creada por operadores del Departamento de Defensa de EU. Nuestros integrantes tienen experiencia inigualable en el ámbito de ciberseguridad, defensa de sistemas, forense digital y desarrollo de soluciones especializadas.

Publishers Note: We caution and caveat the information enclosed as our professional opinions and observations during this engagement and does not attempt to represent the views of the Puerto Rican government. The contents of this case study are not authorized for use in the press, is not suitable for referencing nor serves as testimonial evidence for use in legal preceding's without the expressed notification, consent and approval from Comp Sec Direct LLC.