El trabajador en remoto es secuestrado para pedir un rescate

Los hackers están aprovechando al máximo el cambio de paradigma hacia el trabajo a distancia para atacar una de las mayores vulnerabilidades cibernéticas de las compañías: su capital humano.
Las organizaciones deben permanecer en constante alerta, tomando medidas proactivas y preventivas para identificar vulnerabilidades cibernéticas nuevas y emergentes, asociadas con el trabajo remoto, de modo que puedan prepararse y protegerse frente a ellas.

Los ciberataques han aumentado un **33%** desde el inicio de la pandemia del COVID-19[1]

Más del **50%** de las compañías no estaban preparadas para el trabajo remoto previamente al COVID-19[2]

Los hackers persiguen el eslabón más débil de su organización: los trabajadores remotos[3]

2/3 de los trabajadores remotos carecen de la formación básica y necesaria en ciberseguridad para detectar un ciberataque[4]

Si un trabajador remoto es víctima de un ciberataque, las consecuencias para la compañía pueden ser devastadoras. El año pasado el ransomware supuso pérdidas de más de **€5.5 billones**[5] para las empresas de todo el mundo y probablemente la situación derivada del COVID-19 incremente aún más esa cifra en 2020/21. El siguiente escenario ficticio muestra la facilidad con que se puede desarrollar un ataque de este tipo.

Viernes
Compromiso inicial

16:27 | Carlos está teletrabajando según las indicaciones de su compañía.

17:28 | Carlos recibe un correo electrónico que parece ser de la agencia de viajes corporativa que detalla las acciones urgentes y necesarias a realizar para cancelar los próximos viajes debido a la pandemia.

17:39 | Hace clic en el enlace web presente en el correo electrónico para cancelar su próximo viaje a una conferencia que ha sido pospuesta. Sin darse cuenta de que el enlace es malicioso, Carlos ha permitido, sin saberlo, que atacantes de ransomware altamente capacitados tengan acceso a la red corporativa.

Transcurre todo el fin de semana sin levantar sospecha, los delincuentes comienzan su labor y el ataque todavía no ha sido identificado.

Lunes
El ataque permanece sin ser detectado

09:33 | Carlos se da cuenta de que no puede acceder a algunos archivos de su ordenador portátil. Envía un correo electrónico al equipo de IT y continúa con su trabajo pensando que podría ser un simple problema de conexión.

No sospecha nada inusual, ya que los problemas de IT han sido comunes tras el cambio al trabajo en remoto. Durante el fin de semana, el ransomware se ha extendido por toda la red de la compañía.

17:17 | Carlos termina su trabajo diario y cierra la sesión. Mientras tanto, los atacantes han aprovechado el compromiso inicial para moverse por la red corporativa y acceder a una cantidad cada vez mayor de datos sensibles.

17:29 | El personal de IT revisa el ticket de incidencia de Carlos; han estado ocupados manteniendo los sistemas desplegados para hacer frente al trabajo remoto a gran escala.

17:35 | El equipo de IT envía a Carlos instrucciones para que reconfigure sus conexiones de red y llame por la mañana si el problema persiste.

El equipo de IT se ha ocupado recientemente de varios problemas de conectividad en los que las personas no podían acceder a sus archivos almacenados y este problema no parece ser diferente. Sin acceso físico a su ordenador portátil, el equipo asume que las actualizaciones de red recientes resolverán el problema.

Martes
El ataque es escalado e identificado

07:22 | Los atacantes han tenido tiempo de bloquear cuentas en la red corporativa y extraer datos críticos.

08:00 | Los atacantes movieron ficha, cifraron los archivos y publicaron una demanda de rescate lista para cuando los usuarios inicien sesión.

08:30 | Carlos y sus colegas inician sesión en la red corporativa, encontrando un mensaje que indica que sus sistemas han sido infectados y que pertenecen a un notorio grupo de hackers. Para desbloquear los archivos, los hackers han exigido a la compañía un pago de **€150,000** en una moneda imposible de rastrear. Toda la empresa se paraliza repentinamente, los empleados no tienen acceso a los recursos IT y no pueden operar de forma remota; esto incluye operaciones, proveedores y departamentos de cliente. El equipo de IT (y Carlos) desconocen el origen del ataque. El personal de IT intenta evaluar el alcance del ataque.

Sus archivos han sido bloqueados.
Debe pagar **€150,000.00** para desbloquearlos.

09:00 | Se informa a los directivos de la empresa y se pregunta al equipo de IT sobre cuál es la mejor manera de responder. Se deciden a contratar investigadores y consultores especializados. El CEO solicita actualizaciones cada hora y envía un informe por correo electrónico a la Junta.

09:12 | Un documento de la compañía altamente confidencial se publica, acompañado de un mensaje que indica que se filtrarán más datos en una hora si no se paga el rescate. El ataque es peor de lo previsto, el documento causa un daño significativo a la reputación de la compañía y los teléfonos comienzan a sonar con clientes y socios preocupados por la situación.

09:45 | Los directivos de la compañía se unen a una reunión virtual de emergencia. No saben si pagar ni cuales son las implicaciones. Plantean el tema como una prioridad crítica: ya se han enfrentado a problemas de continuidad debido al COVID-19. Lanzan una declaración pública sobre la intrusión y el CEO se ve inundado de llamadas de los medios de comunicación que quieren saber el alcance real del problema.

15:00 | El CFO ha realizado un análisis inicial y cree que la empresa no cumplirá los acuerdos con varios proveedores, lo que les repercutirá significativamente. El equipo de ventas ha recibido llamadas de clientes clave que cancelan sus pedidos debido a los informes de prensa; una sensación de pánico se ha extendido por toda la organización.

Hasta que se puedan restaurar los sistemas, la empresa experimentará una pérdida significativa de productividad y retrasos en los pedidos de varios y grandes clientes, que podrían resultar en sanciones financieras y legales.

Siguiente Lunes
Remediación

12:04 | Los especialistas que investigan el ataque identifican el correo electrónico malicioso y lo notifican a los directivos de la compañía. Observaron altos niveles de actividad en la cuenta de Carlos durante el fin de semana, fuera del horario laboral, usándolo para limitar el correo electrónico malicioso. El ransomware utilizado está vinculado a conocidos grupos de ataque avanzados.

13:00 | Con esta información, el equipo de IT puede restaurar algunos servicios básicos a sus empleados. Debido al cifrado, los datos clave se pierden y algunos sistemas permanecen caidos; las personas aún no pueden continuar su trabajo.

14:00 | El CIO informa a los directivos sobre la causa raíz del problema y la solución recomendada. Esto incluye una reconstrucción total de la red y actualizaciones de protección de IT que no estaban presupuestadas. El CEO está de acuerdo en que esto supone una prioridad a pesar del significativo gasto no presupuestado.

15:00 | El CFO informa al CEO y a los directivos sobre el impacto financiero del ataque; es material y significativo. El Director Ejecutivo prepara una sesión informativa para el público y recibe una llamada urgente de la Junta.

Lo que una vez fue seguro puede no serlo hoy

Para ayudar a protegerse contra estas amenazas, las compañías primero deben comprender sus riesgos

Solicite una evaluación de riesgo cibernético online.

[1] www.scmagazineuk.com/impact-first-100-days-covid-19-includes-volume-attacks-33/article/1682476
[2] www.practicebusiness.co.uk/half-of-businesses-arent-set-up-for-home-working/
[3] www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory
[4] www.cisomag.com/66-of-remote-workers-in-the-u-k-lack-cybersecurity-training-research/
[5] www.infosecurity-magazine.com/news/ransomware-costs-may-have-hit-170/