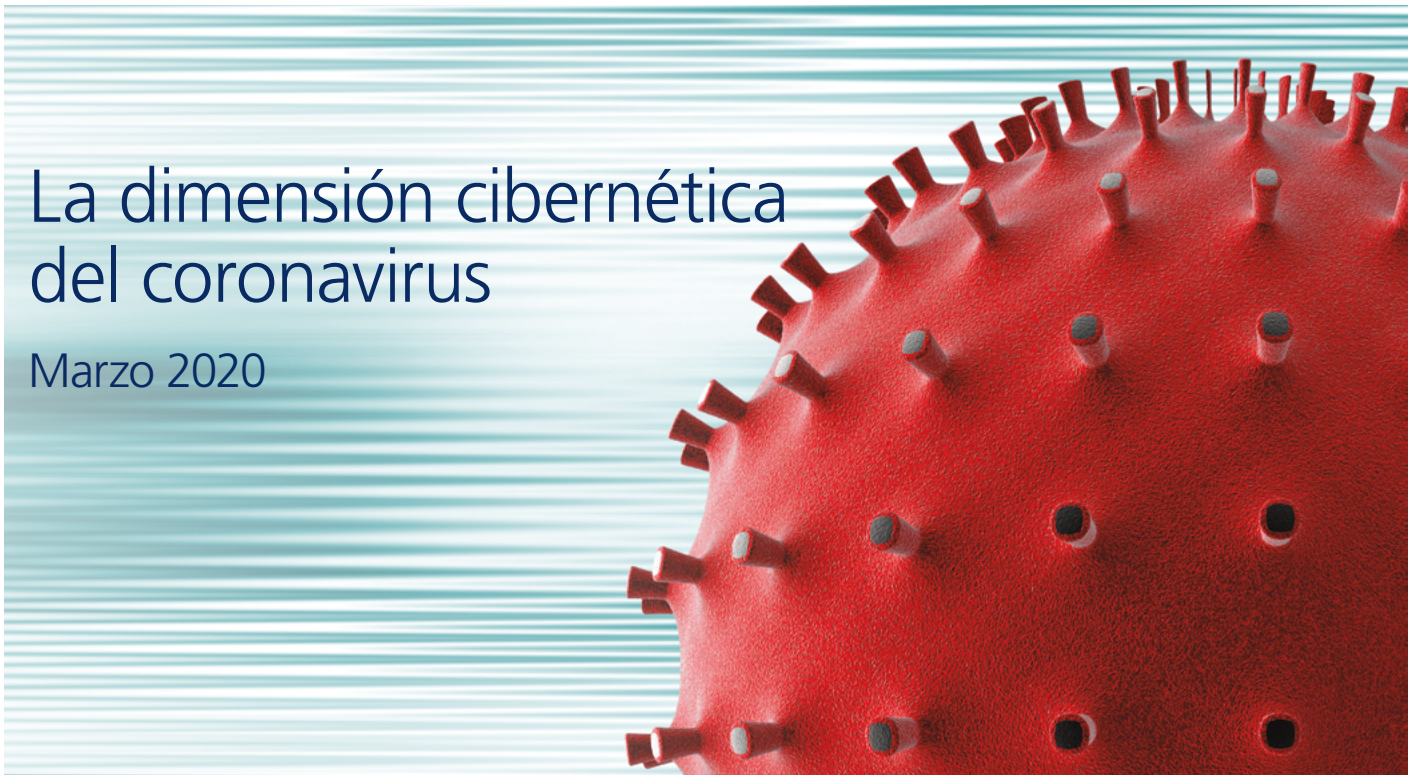
La dimensión cibernética del coronavirus

Marzo 2020



Observaciones

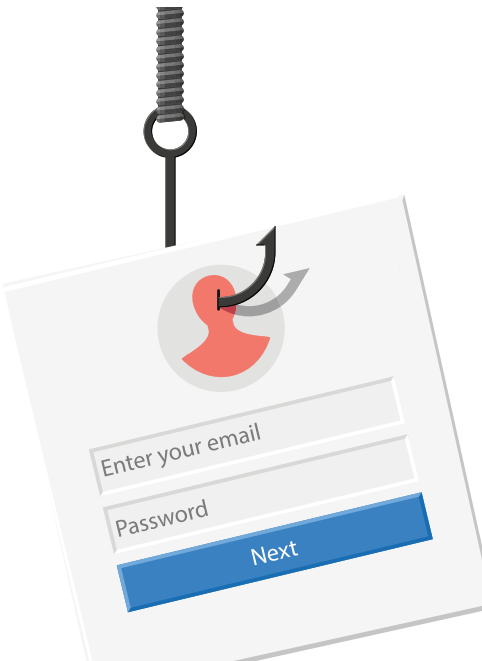
Durante las últimas semanas, se ha producido un aumento extraordinario en el número de incidentes cibernéticos en compañías alrededor del mundo que se han visto afectadas por una nueva ola de ataques cibernéticos relacionados con el tema del coronavirus. Según la firma de ciberseguridad CYE, desde comienzos de febrero los ciber criminales se han beneficiado cada vez más del desconocimiento por la situación causada por esta pandemia global. CYE ha observado un incremento de cinco veces más de incidentes cibernéticos, particularmente en Europa.

Aprovechándose del miedo y de una mayor distracción del público asociada a este evento, existe una probabilidad más alta de que los empleados hagan click en archivos maliciosos o utilicen redes no seguras para recuperar información sensible cuando están trabajando desde casa o en ubicaciones remotas. A medida que las cuarentenas se vuelven más frecuentes y que cada vez más personas están autorizadas a trabajar de forma remota, las empresas deben tener un enfoque multidepartamental para mantener los controles adecuados.

Según estudios recientes, las campañas de phishing y ataques de ransomware han experimentado el mayor incremento en las últimas semanas, debido a que los usuarios hacen click en archivos o enlaces maliciosos que utilizan el tema del coronavirus.

Recientemente tuvo lugar un ataque sofisticado que consistió en hacerse pasar por empleados de la Organización Mundial de la Salud (OMS) solicitando información confidencial, para distribuir un archivo adjunto que robaba información personal.

Figure 1: captura de pantalla de un email de phishing pretendiendo ser de la Organización Mundial de la Salud - Fuente: Proofpoint Inc



[1] https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/amp/

Aumento de riesgos cibernéticos

El trabajo remoto y descentralizado aumenta el riesgo de sufrir los siguientes tipos de ataque:

Phishing / Spear phishing / Comunicaciones Fraudulentas: correos electrónicos u otras comunicaciones electrónicas con información específica sobre el destinatario para engañar al mismo para que haga click en un enlace fraudulento, abra un archivo adjunto malicioso o realice otras acciones comprometedoras.

Business Email Compromise (BEC): correos electrónicos dirigidos a los destinatarios para realizar transferencias electrónicas, generalmente suplantando al CEO, CFO u otros gerentes senior de la organización.

Ingeniería social: manipulación psicológica de personas para realizar acciones que normalmente no harían.

Estos eventos pueden conducir a un mayor riesgo de sufrir un ransomware que puede no solo infectar y bloquear las redes informáticas de las empresas y sus clientes, sino también encriptar o destruir datos. Sabiendo que algunas formas de ataque cibernético pueden permanecer latentes durante días, meses o incluso años, las acciones tomadas hoy podrían tener un impacto significativo en los ingresos y la reputación de una empresa en el futuro. Afortunadamente, existen medidas preventivas que tanto las empresas como los empleados pueden llevar a cabo para evitar estos eventos y mantener un entorno digital seguro y protegido.

Recomendaciones para mitigar riesgos

Personas:

Enlaces / archivos adjuntos: No haga click en enlaces ni abra archivos adjuntos en correos electrónicos de remitentes que no sean de confianza. Si los empleados desean navegar en un sitio web en Internet, se recomienda escribir directamente la URL del sitio que desean visitar. Una URL segura comenzará con https, en lugar de http, pero este criterio no es suficiente: inspeccione cuidadosamente la URL antes de escribirla para verificar que dirige al sitio web oficial de la empresa/institución a la que está intentando acceder. En caso de duda, use un verificador de URL en línea antes de conectarse, como **isitphishing.org**.

Información: No responda ni proporcione detalle de ningún tipo de cuenta a fuentes desconocidas. Las entidades de confianza, como proveedores o vendedores, generalmente ya tienen esta información. Nunca envíe información de identificación personal y/o contraseñas por correo electrónico a personas desconocidas o abra archivos adjuntos en correos electrónicos no solicitados.

Informar sobre actividades sospechosas: Todos los correos electrónicos sospechosos se deben informar al equipo de seguridad cibernética de la organización o al departamento equivalente.

Notificar al Servicio de Asistencia: Todos los empleados deben comunicarse con el Servicio de Asistencia local si creen que han abierto un archivo adjunto o han hecho click en un enlace que pudiera haber infectado su ordenador con un virus o malware.

Empresas:

Formaciones de concienciación de empleados/usuarios: Antes de autorizar conexiones remotas a la red corporativa, los empleados deben recibir capacitación adecuada sobre campañas de phishing y directrices de seguridad, y estar informados sobre todos los procesos y procedimientos corporativos para reportar o notificar un incidente de seguridad si se sospecha o identifica una posible brecha de seguridad o de privacidad.

Conexiones seguras: Utilice solo un acceso remoto seguro a las redes informáticas de la empresa. Donde sea posible, a través de una red privada virtual (VPN), u otro mecanismo de conexión encriptado.

Autenticación multifactor (MFA): Las VPNs deben configurarse con autenticación multifactor como una capa de seguridad adicional para garantizar que solo las personas autorizadas accedan a la red corporativa.

Administración de dispositivos móviles (MDM): Los ordenadores, tablets y teléfonos inteligentes (“smartphones”) de los empleados deben estar equipados con una solución corporativa de MDM. La solución debe aplicar controles de seguridad adecuados y crear un entorno virtual encriptado dentro del dispositivo para almacenar y procesar información corporativa, por ejemplo, documentos y correos electrónicos.

Protección del perímetro de Internet: Los departamentos de TI deben garantizar que los cortafuegos estén configurados correctamente y monitorear el registro del cortafuegos para identificar intentos de conexión o conexiones exitosas de direcciones de Protocolo de Internet (IP) no autorizadas o sospechosas.

Seguridad en la nube y cumplimiento normativo: Las empresas que utilizan servicios en la nube deben garantizar que las configuraciones de seguridad se refuercen y supervisen de manera adecuada para detectar cualquier desviación o alteración de configuración o manipulación no autorizada.

Mayor supervisión y diligencia: Si hay regiones geográficas o países en las que los que los empleados no tendrían razón para conectarse de forma remota a la red de la empresa, el departamento de TI debe poner de forma proactiva los rangos de IP en “lista negra” (‘blacklist’) para esas zonas geográficas de forma que no puedan conectarse de forma remota a redes corporativas.

Consideraciones finales

Es natural enfocarse en las cosas que vemos. El COVID-19 nos recuerda que lo invisible y lo intangible puede tener un impacto mucho más grave que algunos de los riesgos más tangibles que vemos y leemos todos los días (por ejemplo: incendios, robos o accidentes de tráfico). Los riesgos cibernéticos, al igual que sucede con el COVID-19, entran en esta categoría de riesgos intangibles. En los últimos años, hemos visto varios eventos donde virus digitales han infectado ordenador tras ordenador y se han convertido en una auténtica pandemia en un corto periodo de tiempo. El incidente de NotPetya en 2017 fue la mayor de estas pandemias hasta la fecha, afectando a miles de compañías alrededor del mundo, y causando una pérdida económica estimada en US$10 billones. Tal y como está ocurriendo ahora, la higiene es imprescindible para evitar cualquier infección en primer lugar. Parchear los sistemas y lavarse las manos tienen la misma importancia. Aislamientos de procesos y/o entornos aislados ("Sandboxing") y cuarentenas tienen sorprendentes similitudes cuando se trata de manejar un posible contagio.

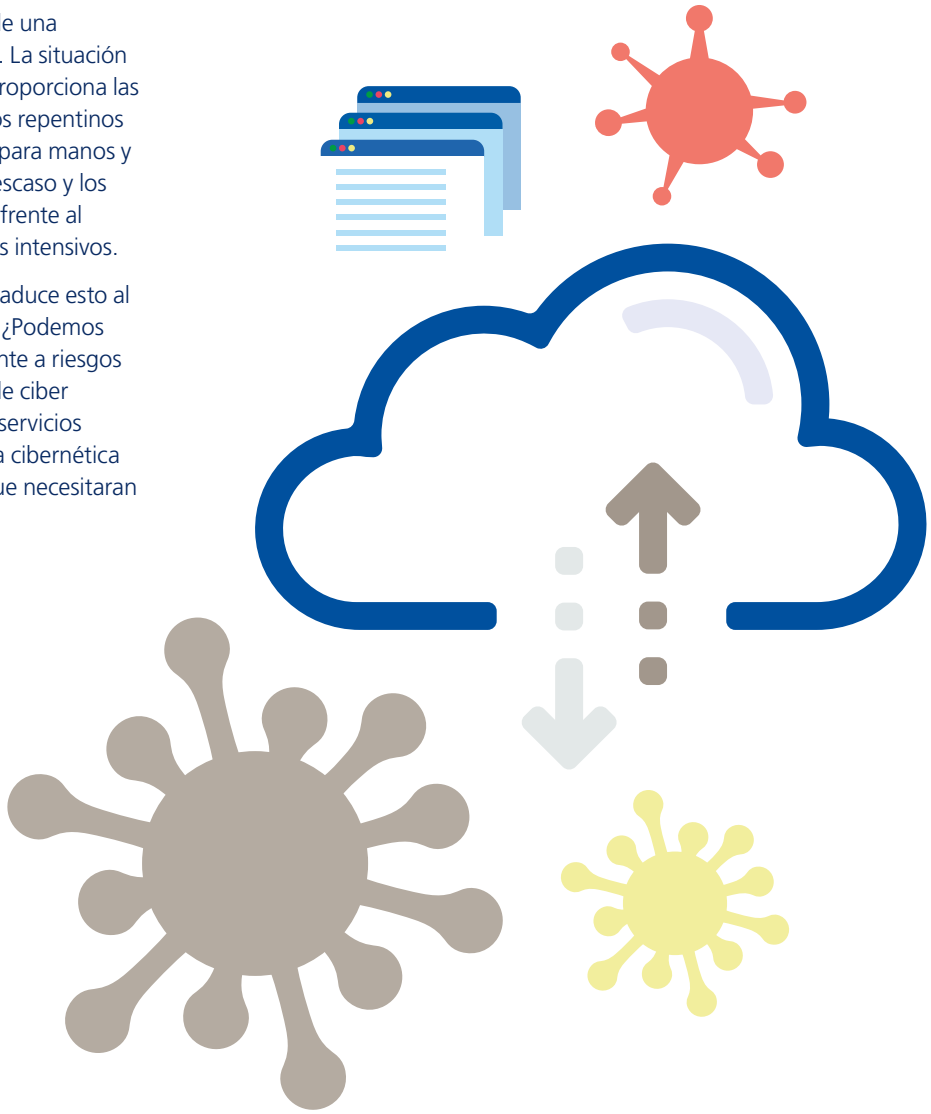
Respecto a los riesgos cibernéticos, el Instituto Nacional de Estándares y Tecnología (NIST) proporciona un marco de actuación para que las empresas fomenten sus capacidades para identificar el riesgo cibernético, proteger, detectar, responder y recuperarse de los ataques cibernéticos. Estas capacidades incluyen tecnología, pero no se limitan a este aspecto. Como se describió anteriormente, la concienciación y los procedimientos conforman el núcleo principal de la protección. Una detección rápida y confiable seguida, cuando es necesario, de una respuesta y recuperación adecuadas es primordial. La situación actual en relación con el COVID-19 también nos proporciona las siguientes ideas: ¿Cómo lidiamos con los aumentos repentinos en la demanda de protección? Los desinfectantes para manos y las mascarillas se han convertido en un producto escaso y los centros y personal sanitario apenas pueden hacer frente al aumento de pacientes en las unidades de cuidados intensivos.

Por lo tanto, deberíamos preguntarnos cómo se traduce esto al entorno cyber y la próxima pandemia cibernética: ¿Podemos confiar en nuestras capacidades de protección frente a riesgos cibernéticos y de respuesta frente a un incidente de ciber seguridad?. ¿Podemos confiar en proveedores de servicios tecnológicos externos en el caso de una pandemia cibernética - sabiendo que dan servicio a muchos clientes y que necesitaran priorizar sus propios recursos escasos?

¿Son autosuficientes nuestras capacidades internas de seguridad informática corporativa y de respuesta a emergencias?

Finalmente, el COVID-19 nos ha mostrado la complejidad de las cadenas de suministro y nuestras dependencias de bienes intermedios de otros países y continentes. Hoy en día, esto no solo es cierto para los proveedores físicos, sino también para los proveedores de capacidad informática, almacenamiento de datos y plataformas en las que operan las aplicaciones.

En las últimas décadas, una tendencia importante en la fabricación ha sido la subcontratación, seguida de la descentralización de servicios. En tecnología de la información, esto no ha sido diferente. Hoy, el movimiento a la nube es el siguiente paso, y muchas empresas están migrando sus infraestructuras de TI a la nube de los grandes proveedores de servicios. La oportunidad técnica de trabajar más eficientemente a través de servicios basados en la nube nos ayuda a responder y recuperarnos de un evento pandémico real, pero también crea la siguiente vulnerabilidad intangible e invisible. Mientras estamos todavía buscando un "interruptor de apagado de emergencia" para el COVID-19, podemos reflexionar sobre lo que ese virus nos dice acerca de nuestra capacidad de resiliencia digital y seguridad cibernética y dónde debemos prepararnos para el próximo virus epidémico cibernético.



173006686 (03/20) TCL

ZURICH®