bakertilly

La ciberseguridad y la era del trabajo remoto

Grandes conversaciones

La ciberseguridad y la era del trabajo remoto

El gasto en seguridad de la información aumentó en 2020 a US $ 123 mil millones, en medio de la propagación de la pandemia COVID-19, pero el gasto en equipos de seguridad de red disminuyó, mientras que hubo un fuerte crecimiento en el desembolso de seguridad en la nube.

Cuando las organizaciones residían en oficinas y ubicaciones centralizadas, los líderes empresariales gastaban miles de millones de dólares bloqueando firewalls y manteniendo los servidores seguros, o deslocalizando sus datos.

A finales de 2019, se estaban invirtiendo más de 121.000 millones de dólares en seguridad de la información y tecnología de gestión de riesgos, y los servicios de seguridad, la protección de la infraestructura y los equipos de seguridad de la red constituían la mayor parte del sector.

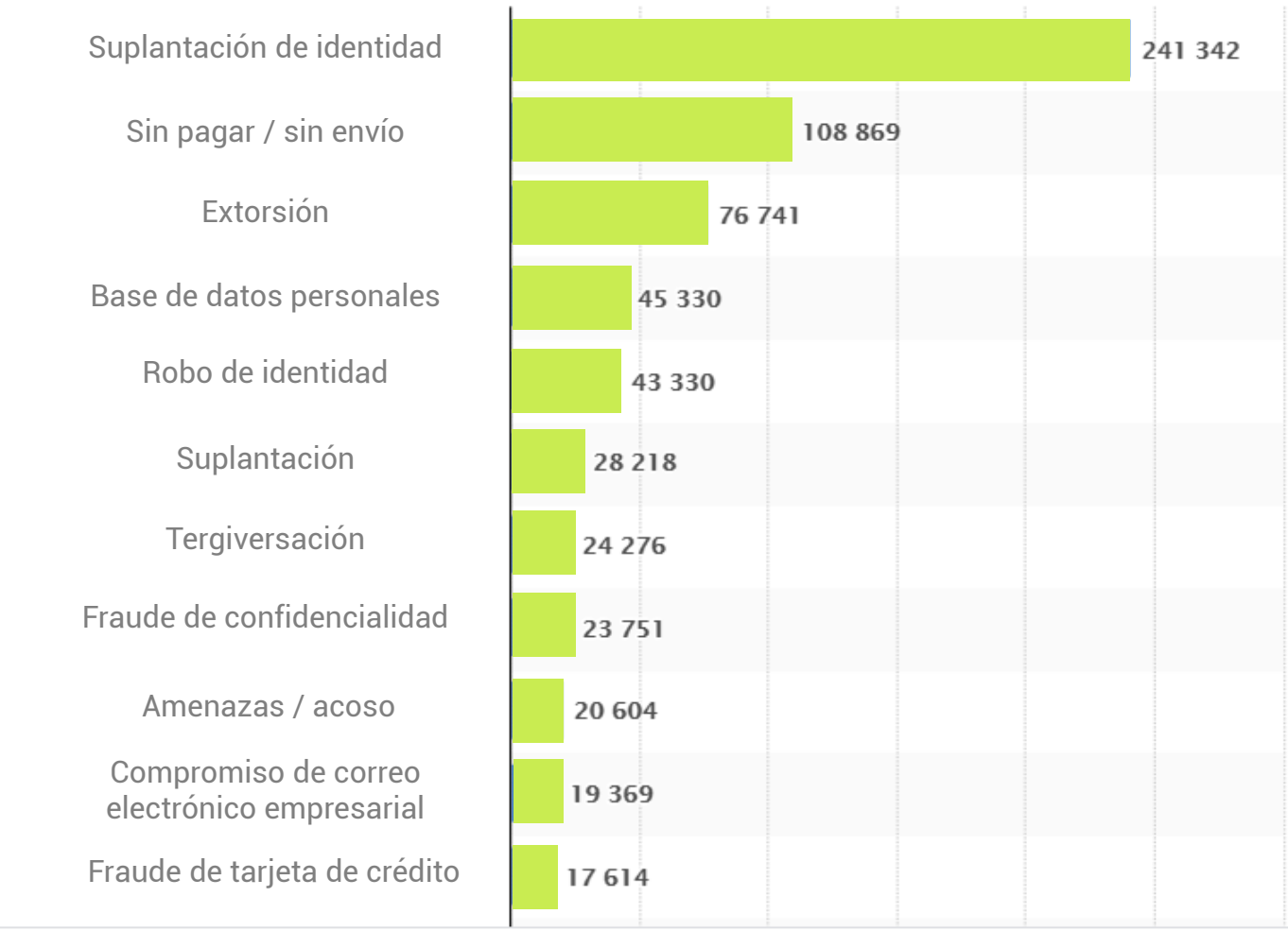
Pero ahora la dinámica ha cambiado. Más del 60% de la fuerza laboral realiza, al menos, parte de su trabajo desde su oficina instalada en casa o desde la mesa de la cocina de su casa compartida, entornos no reconocidos por sus sólidas configuraciones de ciberseguridad.

El gasto en seguridad de la información aumentó en 2020 a US $ 123 mil millones, en medio de la propagación de la pandemia COVID-19, pero el gasto en equipos de seguridad de red disminuyó, mientras que hubo un fuerte crecimiento en el desembolso de seguridad en la nube.

A pesar de este gasto, el ciberdelito se disparó durante la pandemia. Solo en los EE.UU., los presuntos delitos de Internet aumentaron un 69% durante 2020; con todo, desde estafas de phishing hasta ransomware, con un costo estimado de US $ 4,2 mil millones en pérdidas.

Tipos de delitos cibernéticos denunciados con mayor frecuencia al Centro de Quejas de Crímenes por Internet (IC3) en 2020, por recuento de víctimas.

Las pruebas limitadas y los desafíos en la atribución de la causa de muerte, significan que el número de muertes confirmadas puede no ser un recuento exacto del número real de muertes por COVID-19.

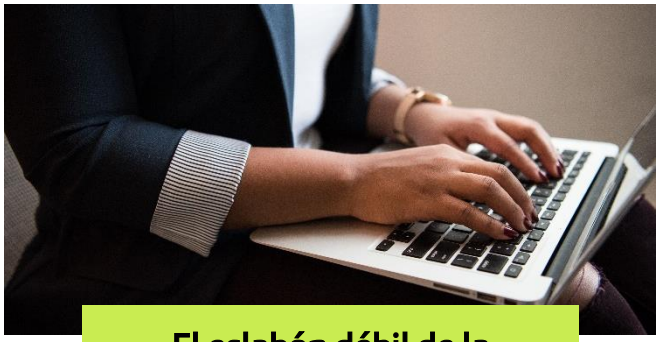


Entonces, es razonable preguntar: ¿la tecnología está fallando en organizaciones cuyos empleados han estado trabajando desde casa o hay algo más?

“Es realmente interesante el trabajo desde casa, porque no es tan difícil como la gente piensa asegurar adecuadamente a los empleados remotos, generalmente es una elección organizacional”, dice Jeff Krull, socio a cargo del equipo de servicios de ciberseguridad de Baker Tilly US.

“Todo el mundo piensa que la seguridad se trata de gastar en tecnología y que la gente está 'pirateando' utilizando estos mecanismos sofisticados realmente locos.

“Pero cuando comienza a reducir algo de lo que realmente sucede en la mayoría de las infracciones, la causa principal es que las organizaciones a menudo se muestran reacias a implementar las medidas de seguridad adecuadas.



El eslabón débil de la ciberseguridad no siempre es la tecnología

Más de la mitad de la base de clientes de Baker Tilly informa una comprensión básica o por debajo del promedio sobre el riesgo de ciberseguridad de trabajar desde casa, según una encuesta reciente que evalúa el impacto de la transformación digital en los clientes.

La prisa por poner a la fuerza laboral a trabajar de forma remota, a menudo se produjo a expensas de la seguridad y los mayores riesgos en el trabajo remoto que las empresas de Baker Tilly vieron entre sus clientes, fueron los ataques de phishing (59,6 por ciento de los encuestados) y el acceso no autorizado (51,1 por ciento).

Un encuestado dijo a la encuesta que la ciberseguridad no era una preocupación principal para los clientes durante el cambio de trabajo remoto, con el enfoque en mantener la producción en marcha, mas que en implementar salvaguardas.

Las organizaciones están tratando de mitigar los riesgos confiando en que el personal cumpla con las políticas de seguridad (60,9%) y aumentando la capacitación del personal (58,7%), así como confiando en sistemas de detección (41,3%) y proveedores externos (39,1%) y el aumento del soporte remoto (39,1%) para identificar amenazas.

Pero el personal solo será tan efectivo como la cultura que existe dentro de la organización. Krull dice que muchas organizaciones que se ven afectadas por la seguridad cibernética y las violaciones de datos, ya conocían las debilidades antes de que fueran violadas.

“Hubo una decisión casi implícita de que 'sabemos que esto es un riesgo, pero no vamos a correr más y más rápido para cerrar ese riesgo'", dice
“De nuevo, en mi experiencia, eso se debe a que eliminar ese riesgo creará algunos cambios en las prácticas del flujo de trabajo empresarial.

Ese es el desafío, el deseo de adoptar buenas prácticas de seguridad.

“Las prácticas en si mismas no son difíciles de encontrar y, desde el punto de vista tecnológico, generalmente no son difíciles de implementar. Se trata de lograr que la gente participe con voluntad, esa es la parte difícil y eso requiere participación de los ejecutivos, no la participación de la tecnología".

Jeff Krull

“Pero demasiados ejecutivos toman el camino opuesto y dicen, no quiero que mi gente tenga que poner un token en su teléfono y demostrar que realmente son ellos, o no quiero limitar quién puede acceder a qué, quieren que las personas puedan utilizar algún sitio para compartir archivos desde cualquier lugar.

"Si su gente puede usar cualquier dispositivo para acceder a ese sitio de intercambio de archivos, adivinen qué, si el malo entra, pueden acceder a lo mismo desde cualquier lugar".

El ransomware está acumulando titulares en todo el mundo a medida que los delincuentes extorsionan con enormes sumas de las organizaciones para desbloquear sus redes informáticas.

Una red petrolera de EE. UU. se vió obligada a cerrar en mayo después de que piratas informáticos irrumpieron en el oleoducto Colonial, lo que resultó en un pago de US $ 4,4 millones para volver a poner la operación en línea.

La prevención de los ataques de secuestro de datos es un asunto serio.

El proveedor de carne JBS pagó un rescate de 11 millones de dólares en junio después de que las plantas de producción que procesan aproximadamente una quinta parte del suministro de carne de EE. UU. Fueran destruidas.

El secuestro de datos o ransomware, es una de las mayores amenazas de ciberseguridad que pueden enfrentar las empresas, dice Marcello Smalbil, director de asesoría de TI de Baker Tilly Holanda, porque las empresas que no están preparadas tienen pocas opciones.

“Es un problema grave, es algo para lo que nuestros clientes deben prepararse y tener las medidas suficientes para evitar que suceda", dice.

"Pero si sucede, deben tener medidas para recuperarse".

Para evitar un ataque de ransomware, los líderes empresariales deben pensar como los malos, porque piensan como una empresa.

> “El ransomware es solo otro modelo de negocio para los delincuentes, y puede pensar en sus objetivos como clientes”.
>
> Marcello Smalbil

“Intentan cifrar tantos clientes como sea posible y luego piden tarifas. Pero lo que es más importante, las tarifas no permiten que la víctima se declare en quiebra.

“Es un compromiso entre pagar el rescate o poder recuperarse a tiempo en un entorno operativo confiable. Es una cuestión de costes. Las víctimas pagan el rescate, cuando es más barato pagar que intentar recuperarse del ataque. Y esa es la forma en que funciona el modelo de negocio.

“Si el rescate era demasiado alto, entonces todos dirían, intentaré recuperarlo de otra manera.

"Pero si el rescate es lo suficientemente bajo, entonces la mayoría de la gente dice que pagará el rescate, luego obtendré la clave y recibiré consejos sobre cómo evitar que vuelva a suceder".

El ransomware se puede prevenir, pero requiere que las organizaciones interrumpan el modelo de negocio criminal, y comienza con el fortalecimiento de la cultura organizacional.

“El primer paso a dar es ser consciente de que puede sucederle a usted y capacitar a su gente y no hacer clic en todo lo que ven en un correo electrónico, entre otros", dice Smalbil.

“También necesita fortalecer sus sistemas, por lo que, por ejemplo, cualquier protocolo o servicio que no necesite para que su operación funcione debe estar deshabilitado".

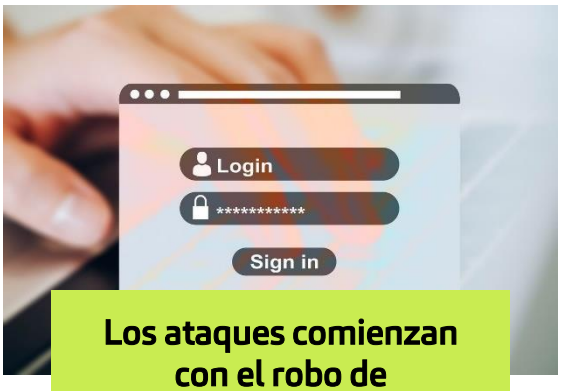
Una estrategia de respaldo también es crucial porque los delincuentes cibernéticos dependen de que las empresas no tengan una o que tengan una vulnerable.

Smalbil sugiere seguir una regla 3-2-1 como una buena guía: establece que las organizaciones deberían tener:

- Tres copias de los datos, una primaria y dos copias de seguridad;
- Dos de ellos deben almacenarse en diferentes medios de almacenamiento;
- Uno debe estar fuera del sitio, físicamente y / o en la nube.

"Sin la copia de seguridad de los datos, las organizaciones se ven paralizadas con muy pocas opciones si son objeto de un ataque", dice Smalbil.

Los piratas informáticos buscan debilidades para ingresar a las organizaciones y, para muchos ataques, comienzan con el correo electrónico y la contraseña de un usuario.



Los ataques comienzan con el robo de credenciales.

Las credenciales comprometidas, es decir, un inicio de sesión y una contraseña robados, representan el 61 por ciento de las infracciones y es la cantidad de ataques de ransomware, como Colonial Pipeline, que se arraigan.

Sin embargo, una buena solución para prevenir el robo de credenciales es simple, dice el Sr. Smalbil.

“Una de las mejores soluciones que se me ocurren es la autenticación multifactor”, dice.

“Vemos muchos clientes que solo usan una identificación de usuario y una contraseña, y siempre recomendamos introducir la autenticación multifactor si es posible porque entonces, todo el problema de olvidar o escribir contraseñas difíciles desaparece.

Krull dice que las organizaciones nunca deberían tener que depender de un único control o protección para evitar que suceda algo malo.

“Si nos fijamos en el ciclo de vida del ransomware, todo el mundo lo ve como, 'alguien entró y puso este ransomware en el que bloqueó las computadoras de alguien'. La realidad es que hay varios niveles que normalmente salen mal para que eso tenga éxito.

“Existe todo este ciclo de vida de controles para prevenir el ransomware, pero inevitablemente lo que escuchas es, oye, alguien hackeó una cuenta y puso este ransomware allí.

"No escuchas que hubo un ciclo de vida completo de controles, que probablemente hay varios niveles de falla antes de que el ransomware tuviera éxito". Muchos líderes de empresas están obsesionados con un área cuando sufren una amenaza o violación de seguridad cibernética y Krull lo compara con un robo en el hogar.

"Si alguien irrumpe y el malo lanza ransomware o lo que sea, entonces la empresa irá directamente a ese lugar y dirá, ahí está, hay una ventana rota con un candado que abrieron, así es como entraron, vamos coloque un poco de madera contrachapada para arreglar esa ventana ", dice.

“Lo que deberían estar diciendo es, ¿tenemos otras ventanas abiertas? ¿Tenemos otras puertas abiertas? Pero no lo hacen, solo se enfocan en esa ventana.

“Cualquier buena organización dirá, déjame revisar todas las ventanas de manera integral, revisar todas las puertas y pensar en lo que estoy haciendo.

“Hay muchas prisas muchas veces después del hecho, y desafortunadamente a veces esas prisas locas son buenas porque existe el apetito de hacer cumplir algunos de esos cambios culturales".

Fuente: www.bakertilly.global

bakertilly
Auditores y Consultores

www.bakertilly.pe
20 – 66 - 700
982 – 881 - 482
noles@bakertilly.pe