
# Riesgos 360º- Episodio 8 - Cómo te ayuda una póliza de ciberriesgos a mitigar un ataque de ransomware

CARMEN SEGOVIA: Siempre se habla del empleado como el eslabón más débil. Esto lo dicen muchos expertos en ciberseguridad. Que a veces es mucho más fácil engañar a un empleado, para que te dé sus claves de acceso al sistema, que no intentar acceder al sistema de la empresa, explotando una vulnerabilidad.

[MÚSICA]

LOCUTOR: Estás escuchando Riesgos 360º, el podcast de WTW, sobre gestión de riesgos emergentes para tu organización.

[MÚSICA]

ALBERTO RODRÍGUEZ: Bienvenidos a Riesgos 360º. Os saluda Alberto Rodríguez miembro del equipo de marketing digital de WTW. Me hace especial ilusión, la temática de la conversación de hoy, porque vamos a inaugurar el apartado de los ciberriesgos. Una amenaza mayúscula para las empresas y en tendencia. Pero que lleva con nosotros más tiempo del que pensamos.

Concretamente el primer ataque de ransomware, riesgo del que trata nuestro espacio de hoy, fue lanzado en 1989. Hace más de 30 años. Para hablar, ¿de qué es esto del ransomware? ¿De cómo proteger a las organizaciones? Y, ¿de cómo ha evolucionado el escenario de la ciberseguridad desde entonces? Se encuentra con nosotros Carmen Segovia, directora en la unidad de ciberriesgos de WTW España. Bienvenida Carmen, ¿cómo estás?

CARMEN SEGOVIA: Hola, Alberto. Muy bien, muchas gracias por la invitación.

ALBERTO RODRÍGUEZ: Muchas gracias a ti, por este rato con nosotros. Vamos a hablar de ciberriesgos contigo, concretamente del conocido como ransomware. Como adelantaba hace un momento, de forma sencilla, ¿podrías contarnos en qué consiste esto del ransomware? Y ¿por qué es una amenaza tan importante para las empresas?

CARMEN SEGOVIA: Pues mira, el ransomware es un tipo de malware o software malicioso, que infecta a determinadas partes o archivos del sistema operativo e impide el uso normal o restringe el acceso a los datos. Porque estos quedan cifrados. El cibercriminal a cambio va a solicitar el pago del rescate, para poder recuperar el funcionamiento y el acceso habitual de los sistemas de la empresa. Es una amenaza importante

para cualquier tipo de organización porque, como ves, al afectar el sistema, la actividad de las empresas suele quedar interrumpida, en el peor de los escenarios, o ralentizada si más no. Con lo cual, esto siempre va a conllevar una pérdida económica, que puede llegar a ser importante para la empresa.

ALBERTO RODRÍGUEZ: Estamos hablando de un secuestro en toda regla. ¿Cuál es la tendencia? Es decir, ¿vamos a más? ¿El número de ataques se ha intensificado en el contexto de la pandemia y de un mayor uso de la tecnología? ¿Qué dicen las cifras oficiales?

CARMEN SEGOVIA: Sí, efectivamente, Alberto. Estamos en una tendencia alcista de este tipo de ataques. Esa tendencia alcista se inicia en 2020, justo en el momento del confinamiento duro. Cuando estábamos todos en casa. Esto hay que ponerlo en contexto. ¿Qué sucede en ese momento? Como todo el mundo tiene que quedarse en su casa y no se puede salir, las empresas tienen que seguir manteniendo, ni que sea un mínimo de actividad, de servicio, con lo cual se implementa deprisa y de forma improvisada lo que es el teletrabajo. Ten en cuenta que, en la mayoría de los países, esto todavía no era tan frecuente. Con lo cual, en muchas empresas los empleados empiezan a conectarse con dispositivos personales, no los corporativos, por lo tanto, el estándar de seguridad de esos dispositivos es menor. Se empiezan a utilizar nuevas herramientas, son los teams, zooms, etc. Es decir, empiezan a abrirse, o sí más no, a crecer en una exposición mayor a que pueda acceder un ransomware, un malware o en cualquier medida tener una brecha de seguridad. Un acceso no autorizado a los a los sistemas.

Ahí es en ese segundo semestre de 2020, cuando se ve una explosión de ciberataques como nunca se había visto antes. Y esto hoy en día continúa. Y continúa, porque además el ransomware nos lleva a distintas derivadas. Cada vez se sofística más, es decir, si en un inicio, años atrás, lo que había era un secuestro de los datos y se te pedía un rescate a cambio, ahora ahí puede empezar el primer ataque de ransomware. Ese mismo ransomware, el cibercriminal, además de pedirte el rescate para descifrar los datos, te puede pedir un segundo rescate. Porque te puede estar amenazando con que, como ha conseguido acceder y copiar esos datos, esa información, te puede amenazar con hacerla pública, divulgarla o con venderla a un competidor. Puede amenazarte también con colapsarte los sistemas. De manera que...

Exacto, ahí está, la interrupción de tu actividad se pueda ver perjudicada durante muchas más semanas. Es decir, esto nos viene a poner un poco en situación como el riesgo tecnológico, es un riesgo de negocio. Y luego es muy curioso también, porque en esta sofisticación que te cuento, Alberto, que está teniendo el ransomware, empezamos a ver también ataques dirigidos. Y aquí te voy a contar una anécdota, bastante curiosa, que pasó en 2019.

En 2019, desde un puerto en Sudamérica, parte un carguero hasta arriba de aguacates. Y que tiene, parte del carguero desde un puerto en Sudamérica para llegar al puerto de Nueva Jersey. Unas millas antes de poder entrar al puerto, ese carguero, o la naviera propietaria del carguero, recibe un ransomware. El carguero, los sistemas se apagan como consecuencia de este ransomware. Y a la naviera, nadie contacta con la naviera. Es decir, claramente los indicios es que eso es un ransomware, y hay que dar un poco a la espera de que el cibercriminal se ponga en contacto para exigir pago del rescate. Obviamente la naviera y la tripulación del carguero intentan resolver la situación, pero no pueden hacer absolutamente nada. Ten en cuenta también que la...

ALBERTO RODRÍGUEZ: ¿Se quedaron varados en medio del mar, bueno a la entrada?

CARMEN SEGOVIA: Exacto, porque además la autoridad portuaria, no claro ante esta situación, no dejaba al carguero entrar en el puerto y atracar. Porque claro tú no sabes a lo que te expones. Con lo cual, se tiene que quedar unas millas adentro, completamente parado, hasta ver qué pasa. Empiezan a pasar los días, el cibercriminal no se pone en contacto con la tripulación, ni con la naviera.

ALBERTO RODRÍGUEZ: ¿Ni con el propio buque?

CARMEN SEGOVIA: Exacto, y, además, acuérdate que esto era un cargamento de aguacates. Los aguacates empiezan a pudrirse. Total, en resumidas cuentas, pasados unos días, el buque, sin saber ni cómo ni por qué, los sistemas vuelven a funcionar. Con lo cual, ahora sí la autoridad portuaria autoriza el atraco de la embarcación. La embarcación llega a puerto. La mercancía no se puede aprovechar. O sea, se tienen que tirar los aguacates, no sirven de nada. Y es en la investigación posterior intentando aclarar qué es lo que ha pasado, que los únicos indicios o las únicas sospechas nos llevan a pensar que fue un ataque dirigido, para intentar influir en el precio de los aguacates en el mercado estadounidense. Había una sobre oferta de aguacates, estaba cayendo el precio del aguacate y probablemente se cree que fue un ataque dirigido para incidir en precio del mercado. O sea, imagínate.

ALBERTO RODRÍGUEZ: Hasta dónde llegan las consecuencias. Hasta dónde llegan las consecuencias, porque solo vemos la cabeza visible, que es el ataque. Pero entonces, Carmen, dentro de esta vamos a llamarla la disciplina de la ciberextorsión, que cada día está más, es más sofisticada. Además de este ejemplo que me has puesto, por protocolizarlo de alguna manera, ¿cuáles son o cuáles serían las técnicas más frecuentes o de mayor tendencia, que se pueden esperar para lo que nos queda de 2022 y los próximos años?

CARMEN SEGOVIA: Bueno aquí, como te decía, la tendencia sigue siendo alcista. Estamos viendo nuevos tipos de ransomware, no solo por el propio software, sino también por la dinámica que adquiere el pedir del rescate. Lo que te comentaba de la doble extorsión, del ataque dirigido o incluso también, tengamos en cuenta que estamos hablando ya del ransomware as a service. Es decir, un software que se vende ya como un producto que cualquiera puede comprar y lanzar un ciberataque.

En este sentido pasamos a tener organizaciones que se encargan solo de desarrollar ese software malicioso, que se pone a la venta de otras organizaciones. Que lo que hacen, es adquirir ese software y ellas mismas se encargan del envío masivo. Generalmente esto siempre se hace un envío masivo, y es ahí en ese volumen donde siempre habrá gente que picará, clicará y el malware podrá acceder a los sistemas encriptando, que es lo que buscan. Entonces, esta segunda organización se encarga más de la gestión del software malicioso y del cobro del rescate. Con lo cual, como ves aquí, son grupos mafiosos, cibercriminales, que entre ellos se apoyan de esta manera para lucrarse. Es que al final esto es un negocio muy lucrativo.

ALBERTO RODRÍGUEZ: ¿Entonces, me estás diciendo que existe hasta un mercado, por decirlo así, en el que se comercializa con este tipo de productos? ¿Y ya no hace falta que tú dispongas de un especialista en tu equipo, que es el propio desarrollador, sino que ya tú puedes comprar ese paquete de software as a service, igual que lo podríamos hacer con otro tipo de herramientas legítimas en mercado? Hemos hablado de esta extorsión, de la ciberextorsión. Hemos hablado de este ataque de ransomware dirigido. Ahora mismo acabas de comentar también el auge del ransomware as a service. Con este múltiple frente de amenazas, ¿cómo pueden protegerse las empresas ante ellas? Porque cada vez este tipo de ataques o de amenazas, son cada vez más avanzados y se distribuyen con mayor facilidad.

CARMEN SEGOVIA: Aquí hablando concretamente del ransomware, en primer lugar, es importante que las organizaciones cuenten siempre con copias de seguridad actualizadas y bien protegidas. Es decir, aseguradas, segmentadas muchas veces e incluso tener copias almacenadas en offline. Es decir, fuera de la red. Esto es fundamental porque, como hemos dicho anteriormente, el ransomware al final no deja de ser un malware que te va a cifrar la información. Si tienes copias de seguridad, que no han sido cifradas, porque están bien protegidas, bueno pues a lo mejor la pérdida económica de la empresa no es algo tan grave, en tanto en cuanto es y elimino todo lo que tengo cifrado e instalo de nuevo las copias que están bien, que están sanas y se pueden volver a utilizar.

Luego, importante, el refuerzo de lo que es la autenticación para acceder a los sistemas con un doble o múltiple factor. Ya que esto al final siempre va a dificultar en mayor medida el acceso no autorizado a los sistemas por parte de los cibercriminales a la hora de lanzar estos ciberataques. Evidentemente no es un sistema infalible, pero si ayuda y protege mejor las puertas de la organización. Es mejor que no tenerlo. Luego...

ALBERTO RODRÍGUEZ: Es un filtro más de seguridad, al fin y al cabo.

CARMEN SEGOVIA: Eso es. Luego, es fundamental también, y ahí se pone mucho foco desde ciberseguridad incluso desde el mercado asegurador, la formación y concientización a los empleados. Que los empleados sepan identificar los mails fraudulentos e incluso que adquieran una disciplina de cautela. Siempre se habla el empleado como el eslabón más débil, esto lo dicen muchos expertos en ciberseguridad. Y es que incluso muchos expertos en ciberseguridad, lo que también nos dicen, es que a veces es mucho más fácil engañar al empleado para que te dé sus claves de acceso al sistema, que no intentar acceder al sistema de la empresa explotando una vulnerabilidad. Esto es así, es cierto hay mucho trabajo de ingeniería social, para poder engañar.

Luego, importante también, porque además es tal la frecuencia que hay de ataque ransomware, que el hecho de que las empresas puedan contar con planes de respuesta ante estos incidentes, incluso planes de recuperación de desastres, es lo que les va a permitir a las organizaciones el enfrentarse de forma eficaz frente a estas amenazas, y poder mitigar y contener las pérdidas económicas que de ellas se deriven. Es decir, que al final ya sabemos a estas alturas cómo funciona un ransomware y qué hace. Estate ya preparado, ten un plan de respuesta que te ayude a esto, a solventar esa situación en poco tiempo. El plan de respuesta que va a pasar desde los backups bien protegidos, a qué personas tienen que actuar en un primer momento para cerrar esa brecha de seguridad, desconectar los equipos infectados, poder prever o identificar la información que se ha visto comprometida, etcétera. Es decir, que esto es fundamental.

Y, por último, importante también, contar con una póliza de ciberriesgo. En este sentido, la póliza de ciberriesgo, la entendemos como una herramienta de mitigación, es decir, en esta gestión del riesgo cibernético, la póliza al final nos ayuda a cerrar el círculo de esa gestión. Es decir, que al final la póliza lo que nos va a ayudar es a absorber la pérdida económica que se derive de ese ciberataque y salvaguardar el balance de la sociedad. Esa pérdida que podría impactar contra el balance, la cuenta de resultados, pues queda protegida por la póliza.

ALBERTO RODRÍGUEZ: Bueno pues me quedo primero con esa reflexión que comentabas. De que los empleados efectivamente pueden ser uno de los eslabones más débiles. Ya no incluso por la falta de conocimiento o ingenuidad, sino porque muchas veces en el ejercicio del día a día, uno va a lo mejor muy frenético, hace una lectura diagonal y a lo mejor no presta la debida atención. Y me gustaría para terminar lanzarte la última pregunta de esta conversación. Hacías referencia hace un momento a la póliza de ciberriesgo, y yo quería consultarte, también para nuestros oyentes. ¿Cómo nos puede ayudar, a mitigar concretamente un ataque de ransomware, gracias a este tipo de póliza que es específica a ciberseguridad o para ciberriesgo en este caso?

CARMEN SEGOVIA: Pues bien, aquí te diré, Alberto. Basándonos un poco en nuestra experiencia en la gestión de siniestros vinculados a ransomware, siniestros que gestionamos bajo estas pólizas, vemos como llegan a ser muy útiles en un primer momento. Porque estas pólizas tienen una cobertura de primera respuesta. Yo te hablaba antes del plan de respuesta a incidentes, hay organizaciones que tienen esos planes de respuesta ante incidentes, pero hay muchas organizaciones que todavía no los tienen. Entonces ahí puedes activar la póliza empezando por esa primera respuesta, que actuaría en ese sentido, tanto si no tienes plan de respuesta incidentes como si lo tienes. Dado que refuerza y aquí te va a ayudar a coordinar

esa primera respuesta a los distintos agentes que tienen que intervenir, ayudar a la organización a gestionar la situación. Desde el forense o los expertos en ciberseguridad, que tendrán pues esto, que ver por donde accedió el ransomware, cerrar esa brecha de seguridad, valorar si hay que desconectar equipos, qué información se ha visto comprometida, etc. Si hay datos de carácter personal comprometidos, pues bajo la primera respuesta vamos a tener el asesoramiento legal para poder cumplir con las obligaciones que establece nuevo reglamento en materia de protección de datos. Ahí ya estamos viendo y hay que notificar al regulador, hay que notificar a los titulares de los datos.

Sí, ese ataque de ransomware llega a los medios de comunicación, porque a veces lo hemos visto, y la empresa se siente pues esto, está un poco hoy en ojo del huracán en los medios de comunicación. Y vemos que aquí puede haber un daño reputacional, un daño a la imagen de la marca. La póliza también va a cubrir, bajo la primera respuesta, lo que sería la coordinación y los gastos de un experto en comunicación. Que te ayude a lanzar una campaña para minimizar el daño la imagen. Con frecuencia, vemos también que, incluso, aun estando la organización preparada para hacer frente al ransomware por esos planes que decíamos de respuesta, de recuperación de desastres, etc. Es inevitable no ver que la actividad queda ralentizado e incluso interrumpida durante días o semanas. Entonces aquí a menudo lo que vemos es que hay una pérdida de beneficios o una caída de ingresos como consecuencia de esa interrupción. Con lo cual, ahí ya tienes una pérdida económica que va a ser importante en muchos casos. Y de esa situación, también luego la organización, la empresa, va a tener también que asumir elevados costes extras que decíamos. Desde las horas extraordinarias de los empleados de los departamentos de IT o de seguridad en sistemas, que pasan a trabajar a destajo. A el tener que, a lo mejor, alquilar provisionalmente servidores para intentar mantener un mínimo de actividad con la que dar servicio a tus clientes. O un alquiler de equipos, etcétera. Esto puede acabar siendo una pérdida económica importante y además cuando la organización tiene contratada una póliza de ciberriesgo, justamente esa es la partida de mayor impacto en la póliza y que muchas veces acaba consumiendo el límite contratado.

Y luego, no olvidemos, a aparte de que la póliza también puede llegar a pagar lo que es rescate, si finalmente la empresa toma esa decisión. Hay que tener en cuenta que esta situación que sufre la empresa puede llegar a ocasionar un perjuicio económico a terceros. A sus clientes, proveedores, usuarios y por ahí pudiera haber reclamaciones por parte de estos perjudicados. Con lo cual, ahí la póliza, aunque esta es una cobertura que se activa pocas veces, eso es cierto, hoy por hoy se activa poco, pero sí que alguna que otra vez hemos visto activarla, la póliza por ahí te va a cubrir gastos de defensa y la posible indemnización al tercero perjudicado. Esto en caso de que sea responsable legal de la pérdida que le ocasiona este, por poner un ejemplo. Así que como ves, Alberto, al margen de lo preparada, de lo mejor o peor preparada que pueda estar la empresa para hacer frente a la situación del ciberataque, la póliza al final es una herramienta necesaria.

ALBERTO RODRÍGUEZ: Escuchándote comprendo que es todo un proceso, es toda una cadena de repercusiones, que tiene muchísimos frentes, y aunque estemos hablando de una herramienta de mitigación, pero esta herramienta de mitigación del daño ocasionado o incluso del riesgo, anticipándonos, unido a ese plan que comentabas antes, a ese plan de recuperación del desastre, son sin duda la mejor arma para mantener a una organización protegida frente a esta amenaza. Pues, Carmen, muchísimas gracias por tu tiempo con nosotros y por todo lo que nos has explicado. Es fascinante, si se puede decir así, como una disciplina que existía en el mundo offline, se ha traspuesto al mundo online.

CARMEN SEGOVIA: Exacto, así es, Alberto.

ALBERTO RODRÍGUEZ: Seguro que volvemos a tenerte en breve con nosotros, para seguir hablando de ciberriesgos.

CARMEN SEGOVIA: Pues será un placer por mi parte, Alberto. Volver a tener una charla de este tipo contigo.

ALBERTO RODRÍGUEZ: Claro que sí, te esperamos. Y a los que nos escucháis ahora mismo, gracias igualmente por vuestra atención y esperamos que hayáis encontrado interesante el episodio de hoy. Y os esperamos, como siempre, en una nueva entrega de Riesgos 360º. Hasta pronto.

LOCUTOR: Gracias por escuchar Riesgos 360º. Recuerda que puedes encontrar más contenido sobre gestión de riesgos en nuestro **blog WTW Update** y en nuestro canal de **LinkedIn** y **Twitter** de WTW España. Anticípate y convierte el riesgo en un camino hacia el crecimiento.

[MÚSICA]