Transformemos Puerto Rico Podcast

Bienvenidos a Transformemos Puerto Rico, el Podcast de Microsoft. Un nuevo espacio para hablar del contexto local, las últimas tendencias y el rol de la tecnología en la transformación del país. Este podcast intentará extender la misión primordial de Microsoft a todo Puerto Rico: empoderar a cada persona y organización para conseguir todo lo que se proponen y más. Abordaremos los episodios con la perspectiva de cómo la tecnología, la ciberseguridad y la Inteligencia Artificial permiten acelerar procesos de transformación digital, recuperación económica y diversidad e inclusión. El episodio de hoy se llama: "Seguridad en tiempos de pandemia", un tema fundamental para cualquier organización en los tiempos que corren. Según la encuesta elaborada por Microsoft, con más de 800 líderes de negocios, brindar acceso remoto seguro a recursos, aplicaciones y datos es el desafío número uno del área. Para hablar de este tema tan importante, tendremos como invitados a Carlos Perez, Practice Lead Research and Trustedsec, quien ha sido galardonado con el premio MVP de Microsoft, para la administración de centros de datos en las especialidades de Seguridad Empresarial y Powershell, durante los últimos siete años. Y a Julio Ureña, especialista de seguridad en Microsoft Caribe. Julio es líder de la comunidad de red Team RD y embajador de HTV, tiene su propio blog y canal de YouTube, en donde enseña hacking y técnicas de seguridad e informática. Mi nombre es Olivia Goldsmith y esto es Transformemos Puerto Rico, el Podcast de Microsoft, bienvenidos. Carlos, Julio, bienvenidos a Transformemos Puerto Rico, el Podcast de Microsoft. Estamos muy contentos de que estén aquí acompañándonos. Para comenzar, me gustaría preguntarle a Carlos: Carlos, sabemos que los ciberataques han crecido enormemente en el último tiempo. ¿Podrías contarnos cómo es el panorama actual de la ciberseguridad?

Carlos Perez

Sí, el panorama actual, en términos de ciberataques, lo que estamos mirando es un alza específicamente en el área de ransomware. Otra alza específica en lo que conocemos como Business Email Compromise, que son ataques a las plataformas de correo electrónico, tanto en el cloud como locales, y hemos visto que ha habido una transformación donde ahora las gangas que se encargan de hacer esa clase de ataques se han centralizado, están invirtiendo más en herramientas, están invirtiendo más en recursos y hemos visto que, de acuerdo a esa inversión que ellos están haciendo, a su vez, ha habido un alza en términos de casos y en términos de la efectividad que han estado teniendo las mismas.

O sea, que tenemos criminales más sofisticados.

Carlos Perez

Correcto.

Perfecto. Carlos, a medida que la tecnología avanza, los cibercriminales también se sofistican cada vez más. ¿Nos podrías explicar en qué consisten estas nuevas amenazas?

Carlos Perez

En términos de las nuevas amenazas, lo que estamos mirando es que ya, como estamos hablando de que, en promedio, con un ataque de ransomware están ganando alrededor de 1.9 millones de dólares en recompensas contra compañías grandes, están cogiendo gran parte de sus ganancias y reinvirtiéndolas, como lo haría cualquier negocio. Estamos diciendo que ya se han ido de una simple ganga de dos o tres personas actuando como una ganga callejera, a una ganga ya criminal más sofisticada, donde ellos ven que tienen que invertir en sí mismos y lo vemos reflejado en términos de que tan pronto sale una vulnerabilidad, dígase para un parche que hay que aplicar a Windows, a Office o simplemente a un artefacto de VPN, antes veíamos que se tardaban una serie de semanas, quizás meses en tener un exploit para el mismo, para poder abusarlo. Y ahora lo que estamos viendo es que, en razón de horas, a través de la inversión de dinero, tienen recursos, para entonces podrá abusar de los mismos, lo que hace que tengamos que parchar mucho más rápido. Vemos que han adquirido software de protección, para además poder encontrar formas de hacer un bypass del mismo. Lo hemos visto también en términos de infraestructura, inversiones en mejor infraestructura para ellos, de manera de poderse esconder. Recientemente trabajamos un caso donde todo el tráfico, aunque iba directo hacia Ucrania, y cuando nosotros empezamos a ver cuáles eran los indicadores de compromiso, y lo trabajamos con nuestro grupo de inteligencia en la compañía, ellos lo que nos informaron era que todos los IOCs en adición a las herramientas estaban realmente asociados a un grupo en China. Y a través de las investigaciones y de rastreo, logramos ver que simplemente lo que hicieron fue que invirtieron en infraestructura alrededor del mundo, de manera de poderse esconder mejor y hacer más difícil el poder bloquearlos y a la misma vez detectarlos.

O sea que, si entendí bien, no sólo se sofistican, atacan más rápido, crecen en número, se centralizan, en promedio, ganan 1,9 millones de dólares por ataque y encima son escurridizos, se mueven de un lugar a otro, de Ucrania a China.

Carlos Perez

Correcto.

Bueno, con todo esto me queda a preguntarle a Julo: ¿podrías comentarnos de qué se trata la mentalidad Zero Trust que Microsoft utiliza como mantra en este tema?

Julio Ureña

Gracias, Olivia. La mentalidad de "Zero Trust" está relacionada con que nunca nosotros vamos a confiar de dónde viene, digamos, la autenticación, de dónde viene ese acceso, sino que siempre lo vamos a verificar. Entonces, en vez de la mentalidad anterior, anteriormente, en el mundo digital, las organizaciones lo que hacían es que todo lo que está en mi organización, yo confío en eso, porque está dentro de mi organización. Y pasamos de esa mentalidad a nunca confiar en nada, independientemente de donde venga, con la premisa de "siempre verifico, siempre confirmo, siempre te autentico, de dondequiera que estés". Y eso es obviamente, lo que permite a las organizaciones es asumir que puede ya existir una brecha de seguridad y estar siempre monitoreando los accesos, siempre monitoreando de dónde viene la autenticación, quién es la persona, los recursos que está intentando acceder, ¿son a los que tiene acceso? ¿No tiene acceso? Y con toda esa información, el modelo de Zero Trust es, pues, simplemente no confío en nadie, siempre trato de verificarte. Y utilizo toda la información e en ese proceso, para yo poder evitar que a una cuenta que ya ha sido comprometida, como lo mencionaba Carlos anteriormente, que es uno de los principales ataques que estamos viendo hoy en día, que si ya comprometiste una cuenta importante dentro de la organización, yo tenga la capacidad de identificar que esa cuenta está comprometida, para evitar lo que viene después, que es el tema del ransomware, que es el tema de chantaje, de pagar la recompensa, si al final eso es lo que estamos tratando de evitar con el modelo de Zero Trust.

Muy claro. Muchas gracias por tu respuesta. Se habla mucho, además, de usar la automatización de los procesos para mejorar esta eficiencia. ¿De qué manera podría servir eso en el espacio de la seguridad?

Julio Ureña

Bien, mira… Es súper interesante que, incluso hablaba con Carlos, antes de que empezáramos el podcast, y lo que él hablaba conmigo era que él estaba automatizando un proceso de un research que alguien hizo. Entonces, tú ves que el tema de automatización, no necesariamente está volcado a quien defiende, que somos nosotros, o sea nosotros queremos automatizar nuestras defensas para evitar que un ataque pueda entrar fácilmente a nuestra organización. Y si entra, pues podamos detenerlo. Pero también los cibercriminales están automatizando y Carlos lo mencionaba en su comentario. Ellos están invirtiendo, están mejorando sus procesos, están utilizando procesos de automatización mucho más rápidos. ¿Para qué? Para que cuando comprometen una organización, con el simple hecho de que le abriste la puerta, muy posiblemente ellos ya están corriendo procesos automáticos que les van a permitir a ellos obtener información confidencial, tener acceso a sistemas no autorizados. Y obviamente, quizás, lo peor que pudiera hacer un ataque de ransomware. Entonces ahí entra también el tema de defensa: ¿cómo yo, desde el punto de vista de seguridad, puedo utilizar la automatización para mejorar mis procesos? Y yo creo que es algo, al menos a nivel personal, que siempre he tratado de hacer, y a veces yo digo que he sido un poco vago en el hecho de que prefiero automatizar un proceso, que tener que repetirlo muchas veces. Y creo que muchas empresas se han volcado a esto. No solamente, digamos, las empresas que proveen un servicio o proveen una herramienta de seguridad, sino también los ingenieros que trabajan

directamente en las empresas, es interesante que tengan este concepto de automatización muy claro, porque no siempre uno va a estar frente a la computadora para poder hacer clic y evitar un ataque. Hay veces que necesitamos que nuestro intelecto esté volcado en una aplicación que pueda hacer lo que nosotros pudiéramos hacer si tuviéramos, digamos, todo el tiempo. Entonces creo que la automatización juega un rol muy importante en el día de hoy, porque las amenazas crecen muy rápidamente, los ataques evolucionan muy rápidamente y no hay forma de que, humanamente, alguien le tome el ritmo a este tipo de ataques sin que, lamentablemente, seamos comprometidos. No sé si, Carlos, tú quieras agregar algo más.

Carlos Perez

Sí, como tú muy bien mencionas: cuando estos actores atacan, nosotros como defensores que tenemos control del ambiente que se está atacando, en otras palabras nos referimos al "battlespace", el área de combate, si queremos decirlo así, porque estamos hablando de una interacción entre nosotros como organización contra otra, o contra otra persona, nosotros controlamos dos factores bien importantes para el atacante: controlamos qué herramientas son las que va a utilizar, de acuerdo a la tecnología que usamos, y los controles que implementamos, y a la misma vez, de acuerdo a los controles que nosotros implementamos, afectamos el tempo, cuán rápido y cuán eficiente ellos pueden atacar. Al nosotros automatizar por nuestro lado y tener un ambiente o un entorno donde nosotros estamos consumiendo todos los diferentes logs y, a la misma vez, tomando acción sobre ellos, que es el punto mayor que podemos ver de deficiencia en muchas organizaciones, a su vez, yo puedo cogerla ahora mismo, habilitarla a través de GPO, todos los avanzos. Puedo poner sismode, puedo hacer todas esas cosas. Pero si no utilizo una plataforma, dígase, como Sentinel, donde tengo un proceso de automatización con Windows Defender ATP, donde yo le digo: "Aíslame este proceso automáticamente cuando veas toda esta serie de comportamientos", pues entonces lo que les estamos dando es un buffer más grande al atacante, o una ventana de tiempo más grande para que él opere. Pero si entonces yo estoy automatizando, se la cierra.

Julio Ureña

No, es clave porque, o sea, mientras más tiempo un ataque esté en curso, más oportunidades yo, como defensor, tengo de detectarlo. El problema está en que si tú ves estos grandes ataques que ocurren, un ransomware bloqueó todas las máquinas. Eso no pasa de un día a otro. O sea, no, los atacantes comúnmente toman acceso a las máquinas, sino que toman acceso a los servidores. Luego que tienen acceso a los servidores, posiblemente tienen que estar borrando backups para que la empresa no se pueda recuperar y tenga que pagar el ransomware. O sea, hay todo un plan, una estrategia detrás que toma tiempo. Si nosotros podemos detectar, como mencionaba Carlos, en ese timeframe al atacante, entonces pudiéramos evitar el impacto sobre la organización.

Carlos Perez

Y cuándo nos ponemos a ver, la mayoría de los ataques que están sucediendo hoy en día a nivel de ransomware, en la compañía en la que yo trabajo, el 90% de los casos de manejo de incidentes que estamos manejando, son de ransomware, todos tienen un mismo patrón: el atacante entra, decide estar alrededor de dos a tres meses dentro de la red acumulando la mayor cantidad de información y filtrando la mayor cantidad de información, antes de efectuar el ransomware. ¿Por qué? Porque tiene una ventaja o un valor la información que se llevaron y tienen dos ventajas específicas: uno, que puede revenderla en el mercado negro, y la segunda es que la puede utilizar para chantaje para "Black Mail", donde le dice a la persona: "O me pagas la recompensa, o empiezo a sacar todos estos detalles". Ahora los clientes están aprendiendo, y nosotros estamos haciendo ejercicios de Red Team, tuvimos hace poco uno de un banco y otro de una firma de abogados, donde nos pidieron que simuláramos esa clase de ataque. En el caso de la firma de abogados, una vez nosotros logramos entrar. A razón de un par de semanas, logramos ir personalmente a uno de los asistentes de los abogados y logramos tener acceso a las grabaciones de negociación de contratos de ciertos artistas. ¿Qué sucede? Si eso se expone, ¿qué vienen a sacar? Es un impacto tipo mediático bien grande. Si yo fuera un grupo de ransomware... y nosotros simulamos en la clase el movimiento lateral en la red que ellos hacen tan bien, para ver si nos detectaban. Si no me detectaban y yo lograba lanzar mi ransomware, y no hubiera sido una simulación, nosotros le decíamos: "Mira el artista tal, tal, tal, tal, sabemos que tienen esto con esta disquera, con esta disquera y con esta compañía de producción de televisión. Si tú no nos pagas, nosotros sacamos público sus contratos, cuánto están ganando, cuanto son sus regalías". Y hasta, en algunos momentos, se puede mencionar hasta a quién no le agrada o qué no le gusta, lo cual entonces se presta para un impacto mayor negativo para la misma. En el caso del lado de la banca, logramos tener acceso al sistema Swift, después de casi tres meses de operación dentro del banco, sin ser detectado. Y allá, con el Sistema Swift, nosotros podíamos empezar a ver todas las transacciones internacionales, como que también nosotros si hubiéramos querido haber efectuado una transacción internacional, vaciando ciertas cuentas. Y esas son las clases de ataques que estamos viendo. El atacante entra y no es un ataque rápido, en términos de efectuar el daño, pero es rápido en su movimiento y expansión a través de la red para poder conseguir la mayor cantidad de información. O sea que mientras más puntos de automatización y más información logremos recolectar del comportamiento de nuestro ambiente, más fácil se nos va a hacer encontrar esos comportamientos dentro de la red, los cuales no son normales de nuestra operación, de manera que podamos levantar banderas y tomar acción.

O sea, estrategia de guerra pura y dura.

Julio Ureña

Así mismo.

Carlos Perez

Si

Carlos, entonces, déjame preguntarte qué consejos podrías darles a los líderes de negocios que nos están escuchando para reforzar sus políticas de seguridad.

Carlos Perez

Yo diría, la número uno es invertir en su gente. Yo puedo coger ahora mismo y poner un EDR, un antivirus, puedo montar lo último de Microsoft en términos de Sentinel, multifactor authentication y todo, pero si mi personal no está entrenado en cómo usar la herramienta, no conoce bien la herramienta y no conoce bien su entorno, no va a poder sacarle provecho a la misma. Lo segundo es conocer su ambiente.

¿Qué sería?

Carlos Perez

Lo primero es identificar cómo hago dinero con una empresa. Si yo soy una empresa, la cual me dedico a la parte de embarcación, todos mis sistemas que tienen que ver con embarque desde el sacar un contenedor del barco, hasta el sistema de billing y la interacción entre ellos, son lo que debería ser crítico para mí. Y muchas veces lo que vemos es que su enfoque o el enfoque de inversión de herramientas de tiempo de monitoreo, no va en acorde con aquellos activos de importancia del negocio. Y vemos que donde están monitoreando algo que no hace sentido y lo que es el activo de negocio no lo monitorean. Así que yo te diría que la segunda es conocer su entorno bien. Y eso conlleva monitoreo. Eso conlleva a tener logs, en adición a hacer un mapping de mi business strategy, mi estrategia de negocios, a mi entorno de IT, donde todos esos activos de IT figuran dentro de mi entorno de negocio.

O sea, invertir en...

Carlos Perez

Y ya una vez que tienes ese conocimiento, ya puedes tomar mejores decisiones más inteligentemente de dónde debo invertir y qué debo proteger dentro del mismo.

Perfecto. Júlio, ¿cómo imaginas un futuro donde la Inteligencia Artificial esté bien aplicada para la ciberseguridad?

Julio Ureña

Mira, tú sabes que la Inteligencia Artificial todavía es un mundo que nosotros estamos explorando. Y definitivamente, hay gente que todavía no lo entiende. Hay gente que sigue pensando que Inteligencia Artificial es un "if else" muchas veces repetido. Quizás haya un

término un poco más técnico, pero en el mundo de la automatización, por ejemplo, cuando hablamos de automatizar, comúnmente tu programa toma decisiones. Pero las decisiones las toma en base a lo que tú creas, las condiciones que tú pusiste dentro del código. O sea, es algo, digamos que está ya puesto dentro del código. A diferencia de con la Inteligencia Artificial, que esa lógica no la creas tú. La lógica la desarrolla la aplicación. Pero es algo que, digamos, dentro de la ciberseguridad, está en un proceso de evolución. Recuerdo un tiempo en donde aquí, precisamente en República Dominicana, en una institución de estudios de alta tecnología, ellos me invitaron para hablar de Inteligencia Artificial y hacking. No defensa, hacking. Y yo en mi vida había visto Inteligencia Artificial. Te digo, para mí la inteligencia artificial era eso mismo. Muchos y "if else" regados dentro del código y la lógica la creaba yo y no tenía idea de cómo funcionaba la Inteligencia Artificial. Y dije que sí, pues para tener la oportunidad de aprender un poco de Inteligencia Artificial. Resulta que terminé haciendo un programa utilizando Inteligencia Artificial que tomaba, por ejemplo: cuando tú vas a una página web, para tú evitar que un robot la ataque o envíe muchas solicitudes, las empresas usan captchas para evitar que obviamente un robot... Pues, si tú no pones el captcha, pues, tú no eres humano. Entonces, yo creé un módulo de Inteligencia Artificial que tomaba el captcha, lo leía y entonces sacaba el texto y lo ponía dentro de la web. Y de esa forma creé un robot que tenía la inteligencia de poder leer el captcha y ponerlo en ese contexto. Y en ese sentido, leía imágenes de manera particular. Y yo no codifiqué mi proceso de cómo él podía hacerlo. Él lo aprendió con los diferentes algoritmos y es algo súper complejo. Si tú me preguntas, todavía no lo entiendo. Sí, lo vi funcionar y creo que el camino de la Inteligencia Artificial es un mundo en el que, en materia de ciberseguridad, hay mucha información. O sea, nosotros recolectamos mucha data. Ahora, el procesar esa data a veces es dónde cuesta. Y lo inteligente o lo interesante de la Inteligencia Artificial es que tiene esa capacidad de ver lo que nosotros no vemos. Por ejemplo, un analista de un software de ciberseguridad, empieza a ver logs y empieza a buscar patrones. Y esos patrones pueden ser una línea de comandos, puede ser una conexión medio extraña, pero como la inteligencia, o sea, dependiendo de lo que utilicemos para desarrollar esa inteligencia artificial, pudiera tener esa capacidad de ver lo que nosotros no vemos y poder señalar lo inusual dentro de lo que parece usual. Y entonces, es ahí donde esa Inteligencia Artificial nos va a ayudar. De la forma en que Microsoft está abordando el tema de la Inteligencia Artificial, tiene mucho que ver con la solución del Microsoft Defender que no se abarca o no se limita al end point, sino que se extiende a la identidad, se extiende a la nube, se extiende al correo. Y entonces ahora lo que Microsoft dice es: "Ok, yo tengo todas estas fuentes de datos que están alimentando, digamos mi engine, entonces yo voy a utilizar todas estas fuentes de datos para detectar lo inusual". ¿Por qué? Porque ya nosotros como industria de seguridad, sabemos que la evasión de los controles de seguridad es un facto. Va a ocurrir. Carlos se dedica a eso. Tú le preguntas y él te va a decir cómo lo hace. Yo, en mi tiempo libre, también me encanta poder demostrar que un mecanismo de seguridad no es 100% efectivo. Entonces, ¿qué te queda para entonces protegerte? Entonces, ¿eso no es tan efectivo como tú entendías que lo era? Te queda tu capacidad de detectar lo inusual dentro de lo que parece, dentro de lo que...

Parece usual.

Julio Ureña

De lo usual. Exacto. Entonces tú tienes que tener la capacidad de detectar, de responder, pero entonces tienes que hacerlo a tiempo, porque de nada vale que tú digas: "Sí, mira, en los logs aparece lo que hizo el atacante". No. Tienes que detectarlo cuando está sucediendo, porque de otra forma, simplemente estás contando una historia que no pudiste detener. Por eso yo entiendo que la inteligencia artificial, junto con lo que hablamos anteriormente de la automatización, juegan un rol estratégico en toda esta parte de protección para las organizaciones. ¿Por qué? Porque nos ayuda a acelerar el ritmo que nosotros tenemos para poder detectar y prevenir los ataques a tiempo.

Carlos Perez

No solo eso, sino también incurre un costo en nosotros cuando, en mi caso, simulamos los ataques. Nosotros, de momento, cuando entramos a una organización y estamos viendo que tienen Defender ATP, automáticamente asumimos que también tienen a Azure Active Directory Identity Protection. Y eso entonces ¿en qué incurre? En que nosotros tenemos que hacer pruebas de todo lo nuestro en un laboratorio antes de ejecutarlo ahí, porque ambos productos, cuando tú lo pones en conjunto lo que están mirando… Uno mira cómo se comporta la máquina, ¿A qué proceso acceden? Si acaso "else as", el proceso en tu máquina que contiene tus passwords. Y son esta serie de ejecutables. La mayoría de los EDRs, nosotros sabemos que solamente se enfocan en el nombre del proceso. Hay otros productos que se enfocan en nombre del proceso, más el command line y cuál es su partner process. Y eso significa que yo tengo que hacer una inversión de poder simular que, de dónde yo vengo, se vea como ese listado de procesos permitidos. Y es una inversión grande a nivel tiempo, a nivel tecnológico y a nivel operacional, para yo posicionarme, para poder simular eso, para poder simular que soy comportamiento válido en la máquina. Y, entonces, cuando ya tienes Identity Protection, ahora lo vemos en el caso del Active Directory. Ahora si hago un query de Active Directory para hacer unos ataques más conocidos, que es [INAUDIBLE] cuyo cual, a nivel de minuto, me permite tener el password de una cuenta de servicio de alto privilegio en la red. Mucha gente no lo configura bien. Y yo diría que casi todo el mundo no lo configura bien y por eso es que se abusa tanto. Si yo hago una búsqueda por todas esas cuentas de servicios y el query mío de Active Directory lo hago muy abierto, nosotros hemos notado que Identity Protection nos detecta inmediatamente, bien rápido. Y eso para nosotros es un dolor de cabeza. Lo que significa que ahora nosotros tenemos que escoger nuestro servicio, hacer nuestra búsqueda por un servicio en específico y tan siquiera, no lo podemos hacer rápido, porque si no, el Machine Learning dice: "Nadie en su vida pregunta por todos los servicios a la vez en menos de un minuto". Ya tenemos entonces que empezar a hacer una búsqueda de un servicio, esperar 40 o 50 segundos, un minuto o dos, hacer una búsqueda por otro servicio. Lo que antes en un ambiente que no tiene soluciones que utilizan machine learning, yo lo puedo hacer, a razón de segundos, obtener toda la información que yo quiero, en un ambiente donde hay soluciones de Machine Learning como atacantes y puedo detectar las mismas. Significa que ahora me tardo mucho más y esa es una de las áreas donde Microsoft es uno de los top 9 en el área de todo lo que tiene que ver con Inteligencia Artificial. En el mundo existen nueve

compañías las cuales dominan el mercado a nivel de Inteligencia Artificial y Microsoft es una de las tres en Estados Unidos, las cuales lo dominan. Y lo podemos ver específicamente y claramente en los productos a nivel cloud, donde, como muy bien lo menciona Julio, tienen la capacidad, a nivel de procesamiento, para procesar esa data.

Perfecto. Una encuesta de Microsoft reveló que el 31 por ciento de las empresas en Latinoamérica han percibido un aumento en los ataques cibernéticos a partir de la pandemia, siendo la industria bancaria la más afectada. En su experiencia y le pregunta a nadabas a quién quiere responder: ¿qué es lo que más se lamentan cuando suceden este tipo de ataques?

Julio Ureña

Bueno, yo creo que sería la incapacidad de responder al ataque a tiempo. Tú te preguntas, o sea, la mayoría de las empresas que vemos en las noticias que reciben un ataque, tienen seguridad, tienen personal de seguridad, invierten en seguridad. Entonces, cuando al final te encuentras en las noticias, sabiendo que no tuviste quizás la capacidad de responder al ataque, es lo que quizás yo entiendo que es donde más las empresas se lamentan, donde yo hubiese podido detectarlo, pero quizás una mala configuración, un password sencillo, algo evitó que yo no tuviera esa capacidad de respuesta. Y quizás mucho tiene que ver con cosas que mencionaba Carlos como: "Bueno, no estoy invirtiendo en mi personal, quizás no estoy aplicando el monitoreo donde debo de aplicarlo", que son cosas que también digamos pudieran entrar en la ecuación. Pero yo creo que lo que más lamentaría una empresa es no tener esa capacidad o no haber tenido la capacidad de responder a tiempo.

Carlos Perez

Y saca a relucir los problemas políticos internos. Porque, al fin y al cabo, las mejores prácticas de cómo evitar esto, se conocen. ¿Qué tenemos que hacer para evitarlo? Se sabe. Pero la interacción humana dentro de las corporaciones y la política interna dentro del mismo, es el factor limitante a que se implementen las mismas. Y con la pandemia, lo que hemos visto es que se cambió el paradigma a nivel de tú tener todos tus activos dentro de una red que tú puedas monitorear. De momento, todo el mundo está remoto y tú no tienes la capacidad para moverte lo suficientemente ágil y rápidamente para poder hacer esa transición. Aquellas instituciones bancarias o corporativas que sí tienen una infraestructura donde se fomenta la cooperación entre unidades, donde no tienen que ir completamente hacia arriba en el *decision tree*, hasta ciertos niveles gerenciales, para después bajar por el otro lado, para poder efectuar una decisión, sino que entre equipos pueden hablarse, tomar decisiones rápidas, son las que vimos que estaban mejor protegidas. A suponer, yo recuerdo que yo tuve muchos clientes que nos empezaron a llamar, específicamente, con dos áreas. Una: ¿cómo hago un deployment de VPN para todo el mundo? Donde entonces nosotros solo les decíamos: "tristemente, te vas a tener que mover al cloud y vas a tener que acoger una infraestructura tipo Zero Trust, y vas a tener que implementarlas rápido, de manera de poder sufragar el poder tener a todo el mundo remoto, como los estás teniendo ahora y, a la misma vez, tienes que invertir en nuevas

soluciones de seguridad, las cuales reporten hacia la nube, porque tienes usuarios de las casas, que simplemente lo que hacían era que se metían en una página web, ordenaban una laptop y llegaba directamente a la casa del usuario. Y, pero el usuario no tiene VPN, “¿cómo le añado Active Directory?”. “Ah, pues ahora tenemos que hacer un deployment de Azure Active Directory lo más rápido posible”. Y de momento: "Ah, pero es que nosotros nunca hemos trabajado con Azure Active Directory". "Ah, pues ahora hay que aprender Azure Active Directory con un Hybrid Environment". Y, ¿cómo hacerlo? "Ah, pero nosotros no tenemos cómo manejar los desktops". "Ahora tenemos que aprender más a los desktops y no tan solo manejarlos, sino también monitorearlos, para saber qué es lo que está pasando". Porque ahora ya no tenemos ni tan siquiera control físico del activo. "Antes yo podía monitorearlo en mi red y sabía dónde estaba y estaba detrás de una puerta donde yo tenía un key card para poder entrar". Ya no. Ahora están en las casas de todo el mundo. Ahora no tan sólo puede ser el empleado el que la está usando, puede ser el hijo teenager del empleado, puede ser el esposo del empleado, puede ser un cuñado o una tía del empleado, el cual, de momento, está usando es activo. Y Dios sabrá dónde se estará metiendo con el mismo. Y las compañías se han visto forzada a no tan solo reestructurarse política y gerencialmente, sino también tecnológicamente, para poderse adaptar en la pandemia.

Perfecto. Otra de las cosas que había revelado esta encuesta es que, si bien muchas empresas aumentaron su presupuesto en seguridad, solamente una de cada cuatro, cuentan con seguro de riesgo cibernético. ¿Qué creen? ¿Es este seguro algo en lo que deberían invertir?

Carlos Perez

Yo, que he trabajado con compañías que han tenido que usar el seguro, he estado empezando a ver un cambio: número uno, las compañías de seguro, cuando comenzaron, no esperaban... ¿Qué es lo que ellos hacen? Ellos ofrecen una cantidad de dinero. De esa cantidad de dinero, ellos empiezan a recibir intereses del mismo, y ellos prevén que van a tener uno o dos o tres casos en los que los cuáles van a tener que pagar, pero todavía se quedan con una cartera de activos, los cuales van a generar intereses y ganancias. Porque tienen que hacer dinero, como compañía, seguro, para poder sufragarse. No es solo la venta del mismo. No es algo altruístico, tú sabes. No lo estoy haciendo por el bien de mi corazón. ¿Qué sucede? Ahora, con el alza que ha habido de ataques tipo ransomware, el alza y sofisticación de los atacantes al penetrar las redes para el hurto de datos, el uso de las redes para ponerlas a ser crypto mining y que tienen que gastar en manejo de incident response, ha subido. Por ende, las primas de los seguros han subido. Los requerimientos de las primas han cambiado. Antes, ellos no te pedían casi nada. Ahora dicen: "tú tienes un programa de seguridad, ¿cuáles son tus controles? ¿Cómo los implementas? ¿Te auditan? ¿Sí o no? ¿Cómo han sido tus últimas auditorías? Para yo pagarte un caso es seguro. yo requiero que tú, que tú hayas cumplido con los siguientes requerimientos de seguridad" donde antes no te lo pedían. Ahora ha habido un cambio bastante drástico. Yo tuve un cliente, el cual, un hospital se apoderó de toda su red, cerraron todas sus clínicas encriptaron todo. Tenían que echar para atrás pacientes que llegaban a la sala emergencia y enviarlos a otros hospitales porque no podían atenderlos. Y cuando fueron a someter a la

aseguradora, la aseguradora les puso mil y un peros para pagar, porque decían: "pero ustedes tienen esto, ustedes tenían lo otro". Enséñame la documentación de esos procesos que tú seguiste, antes de yo pagarte y que no fuiste negligente. Y entonces decía: "No, pero es que esa documentación la tengo encriptada". ¿Cómo te la voy a dar si entonces no pago para recuperar, para decirte que sí, que yo seguí esos procesos?".

Claro.

Carlos Perez

Y se formó ese dime y dame entre uno y otro

Julio, ¿qué piensas?

Julio Ureña

Bueno, mira, si tú supieras que, directamente, no tengo un caso puntual que pudiera argumentar. Entonces, yo creo que nos pudiéramos quedar con el comentario de Carlos en ese sentido.

Perfecto. Me queda una última pregunta. Finalmente, según una encuesta de Microsoft, solo el 27% de las empresas que implementaron trabajo remoto, su fuerza laboral trabaja exclusivamente con dispositivos de la organización. Si la mayoría está usando sus propios devices para tareas laborales, ¿qué quiere decir esto para el futuro de la administración de la ciberseguridad?

Julio Ureña

Yo creo que, Olivia, debe evolucionar. Definitivamente, hay que replantear cómo lo hacíamos y entender que estamos viviendo una temporada diferente y que no es lo mismo. No es lo mismo tener el control de un device, el control de todo dentro de cuatro paredes o edificios que yo controlo, a que ahora todo el mundo tiene en su casa, como decía Carlos, "la prima mía está utilizando la máquina de la empresa" y que pudiera ser eso un riesgo. Y a veces, que, en muchas organizaciones, la mayoría no usa dispositivos corporativos para tener acceso a esta información. Por lo tanto, tú tienes personas que tienen acceso a recursos confidenciales desde equipos no manejados. Lo que, para muchas organizaciones, simplemente fue un shock. O sea, como yo lo vi al principio fue: las organizaciones querían imitar lo que tenían en las premisas, al entorno remoto. Así que pasaron e intentaron pasar todos los controles que tenían de la forma en las premisas, al escenario remoto. Y eso no se puede. Por eso hay que replantearse la forma en que estamos haciendo la seguridad. En el caso, por ejemplo, de Microsoft, yo que soy un empleado que nosotros trabajamos remoto, hay veces que vamos a la oficina, hay veces que no vamos, o sea, que no estamos acostumbrados a eso. Y ya Microsoft venía evolucionando en ese sentido, donde ya, yo como empleado vivo esa experiencia. Y para

mí es simple, o sea, para mí es sencilla. Yo tengo la posibilidad, desde mi máquina de Microsoft, tener acceso a la información confidencial que manejo, tener acceso a los recursos que utilizo, pero si quiero utilizar mi dispositivo personal, por ejemplo, Microsoft me dice: "OK, tú lo puedes utilizar". Pero para tú utilizar tu dispositivo personal, estos son los requerimientos que tienes que tener. Tú me tienes que garantizar, dentro de ese dispositivo, estos controles. Y, entonces, Microsoft me dice si tú quieres utilizar tu dispositivo personal, esto es lo que yo necesito que tú tengas que hacer. Y de la misma forma, si yo intento entrar a ciertos recursos de Microsoft, desde un dispositivo que no es de Microsoft, pues simplemente, Microsoft me va a decir: "Mira, tú puedes entrar a este dispositivo, pero con un acceso limitado", porque es un dispositivo que yo no manejo. Así que, información confidencial clasificada desde ese dispositivo, tú no la puedes ver. Sencillamente. Por lo tanto, el control se traslada desde eso que yo tenía, que yo controlaba, ese device, yo lo transfiero al servicio, lo transfiero a la información, lo transfiero a la identidad del usuario y no para mí como corporación, o dentro de mi estrategia de seguridad, yo defino qué es lo que yo quiero hacer cuando tú vengas desde un equipo corporativo. Y, ¿qué quiero hacer cuando tú vengas desde un equipo que no es corporativo? ¿Qué quiero hacer cuando tú te conectes desde Puerto Rico, que es desde dónde tú siempre te conectas, y qué quiero hacer cuando tú quieras entrar desde España? ¿Me entiendes? Entonces, ya empiezo a replantear mis políticas, mis procedimientos, mi estrategia de seguridad, para llevar ese control, esa política directa a la información, a la identidad o a ese servicio que yo quiero proteger. Entonces, en resumen, yo entiendo que las corporaciones, las compañías, tienen que replantearse la forma en que lo están haciendo. Yo sé que muchas lo han hecho durante la pandemia, forzosamente, y creo que también ha sido beneficioso, en cierto modo para la industria, de entender que esto es algo que nos puede pasar, que no nos imaginábamos. Todavía cuando empezó la pandemia, yo pensaba que, por ejemplo, aquí en Dominicana, que somos un poquito desorganizados como como país y la gente a veces no hace caso, yo decía: "No, mira, nadie se va a poner la mascarilla aquí, en este país la gente no hace caso". Y al final se hizo, todo el mundo la tiene que usar, porque fueron, digamos, reglas que como nación se empezaron a definir y sanciones, si tú no las cumplías. Así que pasó. Entonces, nadie nos libra de que nos pase otra vez mañana, y hoy yo entiendo que muchas corporaciones ya están adoptando este tema de Remote Work como parte de su "nuevo normal", lo que quiere decir que hay que replantear un poco esta estrategia de seguridad.

Carlos Perez

Y no sé si te recuerdas, Julio, antes de que comenzara la pandemia, ese mismo año, en enero y febrero, tú y yo trabajamos los casos de Business Compromise que sucedieron aquí en Puerto Rico. Y yo recuerdo cuando nos sentamos con todos los diferentes líderes de los diferentes municipios, de las alcaldías, nos sentamos con varias agencias de gobierno, industria privada, y Julio y yo estábamos hablando sobre esos temas, y la cantidad de gente que estaba utilizando artefactos personales era gigantesca. Y entonces Julio les empezó a cubrir la presentación. Yo cubrí el lado de ataque, donde yo simulaba todos los diferentes ataques. Y entonces, Julio les abría los ojos y les enseñaba: "Señora, así es como se salvan de alguien como Carlos". Y le empezaba a cubrir toda la parte de cómo tú manejas los devices

móviles, como tú verificas la política, que el device sea compliant. Y si tu device propio no es compliant, no te doy acceso. No te doy la data.

A mí me pasó

Carlos Perez

Y eso fue abriéndoles los ojos a todos ellos. Y yo te diría que dos meses después nos encontrábamos todo en lockdown.

Julio Ureña

Ya sabes.

A mí me pasó, quise abrir mi cuenta de Microsoft desde mi celular y yo tenía una contraseña de cuatro dígitos, y Microsoft me dijo: "No, tiene que tener seis o no puedes abrir tu cuenta de Teams desde ahí". me hace como argén recién cuando. Cuando te escuché hablar dije, pero esto a mí me suena conocido y claro, a mí también me pasó y me queda por agradecerles. Carlos Julio, muchísimas gracias por su participación. Ha sido muy valioso haber contado con ustedes en este episodio.

Carlos Perez

Sí.

Julio Ureña

Es así.

Cuando te escuché hablar dije: "Pero esto a mí me suena conocido". Sí, claro, a mí también me pasó. Me queda por agradecerles, Carlos, Julio. ¡Muchísimas gracias por su participación! Ha sido muy valioso haber contado con ustedes en este episodio. Nos ha quedado muy en claro la importancia de la ciberseguridad para todas las organizaciones y cómo garantizándola, mejora en la productividad y la colaboración. Gracias también a todos los que nos han acompañado a lo largo de este capítulo. Los invito a sumarse a la conversación en las redes sociales, bajo el hashtag #TransformemosPR. Mi nombre es Olivia Goldschmidt y esto fue Transformemos Puerto Rico, el podcast de Microsoft.