SESIÓN DE CIBERSEGURIDAD E IDENTIDAD DIGITAL, 5 MAY 2020

VIDEO TRANSCRIPT

Accenture Academies Online
BE: Beatriz Escobar
AG: Andrés Gil
AC: Adrià Castany

BE: Buenos días a todos y muchas gracias por conectaros a la sesión de hoy. Damos comienzo a nuestra sesión online, donde vamos a hablar de ciber defensa e identidad digital. Y una vez más, esta sesión queda enmarcada en el proyecto que en Accenture hemos bautizado como Accenture Academies Online, que nace con el objetivo de compartir conocimiento con todos nuestros centros colaboradores, tanto universidades como centros de formación profesional y todos nuestros candidatos en proceso.
Adrián, Andrés, si podéis por favor pasar a la siguiente slide, simplemente para que nos pongáis cara, mi nombre es Beatriz Escobar, llevo ya más de 10 años trabajando en Accenture. Dentro del área de Talent Acquisition, dentro de la compañía mi rol principal es coordinar y poner en marcha acciones de captación de talento junior, con especial foco y relevancia en el programa de prácticas y sobre todo el programa de prácticas de formación profesional y hoy estoy aquí un poco por hacer de moderadora de la sesión. Simplemente por ir dando pie al chat y a los comentarios que vayáis aplicando en nuestro chat y que trasladaré tanto a Adrián como a Andrés, que son realmente los protagonistas de esta sesión, así que sin más, os dejo ya con la parte divertida, con Andrés y con Adrián, yo volveré al final de la sesión para contaros un poquito más acerca de la compañía y hacer un poco de cierre y de puesta en común de todos, así que Adrián, Andrés, cuando queráis.

AC: Gracias Beatriz. Empezamos. Yo soy Adrià Castany y tenemos a mi compañero Andrés con la parte de Digital Identity. Los dos llevamos más o menos 4 años en Accenture, yo en la parte de ciberdefensa, dedicándome todo al mundo de la cibersec, que explicaremos más o menos lo que es, y para que podáis entender a qué nos dedicamos y qué es las cosas divertidas que hacemos, o no tan divertidas para otra gente. Y también la parte de Infraestructure Protection, que también os contaré un poco de qué va. Andrés, si quieres presentarte…

AG: Sí, como decía Adri, llevamos prácticamente 4 años en Accenture, empezamos casi al mismo tiempo. Yo he estado siempre dedicado a todos los proyectos relacionados con la identidad digital. Como ha dicho él, ya comentamos en detalle en qué consisten, pero montar una infraestructura de control de autenticaciones y autorizaciones de usuario, en distintos clientes de Accenture, y si queréis empezamos y os vam0os contando un poquito.

AC: Vale, dentro de Accenture, nosotros

pertenecemos al grupo de Accenture Security, que es una subrama que hay dentro de Accenture, que solo se dedica a seguridad y ciberseguridad.

Tenemos oficina en prácticamente todo el mundo, esto es, por ejemplo, un mapa de las que había creo que hace un par de años, aquí hay algunas nuevas que han salido, algunas pocas. En España estamos en Barcelona, que es donde estamos Andrés y yo, estamos en Madrid y estamos en Bilbao, y hay distintos cyber fussions o centros de tecnología repartidos por todo el mundo. En cifras, os las contamos un poco más o menos, qué es Accenture Security a grandes rasgos, para que sepáis dónde nos movemos. Tenemos más de 20 años de experiencia, facturaciones bastante grandes… Lo que os comentaba, de centros de formación o centro Cyber fusión por todo el mundo, centros de delivery, o laboratorios donde simplemente hacemos pruebas, para después presentárselas a los clientes. La idea es que por ejemplo en laboratorios, que en España tenemos uno, en Cloud, para hacer todas demos que queramos, todas las pruebas, romper todo lo que queramos y así, probar todos los productos antes de implantarlo en un cliente.

¿Cómo nos dividimos? Nosotros en Accenture Security tenemos 3 grandes bloques, que es Cyberdeffense Services, Applied Cybersecurity Services y Managed Security Services. Si os fijáis yo estoy en el primero, Cyberdeffense, y Andrés está en el segundo, Applied Cybersecurity, que son las dos más importantes. El tercero es de los bloques que hay anteriormente, pues cómo los aplicamos a nivel de servicio. Me explico. Los dos primeros son proyectos cortos o proyectos que emprendemos en una compañía y después, cuando queremos hacer un servicio, que es un proyecto largo o que quieres implementar a lo largo del tiempo, por ejemplo, estar controlando un servicio, un software, cualquier cosa, sería un servicio.

En el de ciberdefensa, pues fácilmente podéis ver Advance Attack, Application Security, temas de forense, temas de Cyber Pression &Resilience… Más o menos, ¿qué es? Pues en cyber investigation forense, ¿qué hacen? Se dedican a investigar una vez tenemos un ataque y hay evidencia y hay que hacer un forense, igual que se hace en un cuerpo o en la policía, pues lo hacemos nosotros para investigar fácil dónde se ha producido, qué ha pasado, por dónde ha entrado el bicheo, el atacante, cómo ha sido, etc. etc. Y después, una vez hemos investigado, cómo responder para que no nos pase a futuro. ¿Cómo prevenimos también? Hacer un forense es cuando ya te han atacado, pero igual quieres evitar que te ataquen desde el principio, pues Threat Intelligence o con Operations & Resilience, pues cómo actuamos cuando se está produciendo un ataque o en Threat Intelligence pues todas esas evidencias previas que podemos nosotros tener para parar un ataque, me explico. Yo tengo una máquina, un PC, por ejemplo, el de Andrés, que se está conectando a IPs de Rusia o IPs de China, eso huele mal, igual es que tiene algún virus o algún… o cualquier cosa en el ordenador, con lo que podemos pararlo antes de que le hagan daño.

¿En Applied Security? Pues es todo el tema de cómo configuramos el mundo Cloud, estamos migrando cada vez más infraestructuras al mundo Cloud, y las premisas de seguridad son las mismas, pero la forma de activarlas o configurarlas son un poco distintas, porque hay un mundo totalmente paralelo en Cloud. La data security, todo lo que es la protección de la información, los datos son muy importantes y los datos, nos referimos tanto a vuestras tarjetas de crédito como al mail o cualquier dato personal o cualquier dato de empresa, hay que protegerlo. Sabéis que hay normativas nuevas de GDPR, que entraron en vigor el año pasado y una serie de premisas que hay que cumplir, para la privacidad de los datos. Tenemos solo un apartado dedicado a eso, a cómo evito que no roben datos, pero no solo eso, sino cómo evito que se exfiltren los datos, el robo de datos más común no es un ataque externo de que un chino se me ha colado o alguien desde China se me ha colado a nuestros sistemas, sino que son robots internos, es decir, que yo he perdido, estoy trabajando en una empresa, tengo datos confidenciales, y he perdido unas hojas con información clasificada o, adrede, quiero pasar información a la competencia. Pues como evito, el data lost prevention, que todos esos casos ocurran.

El tema de digital Identity, que explicaremos con más detalle con Andrés, después platform security, que es la seguridad que aplicas dentro de una plataforma, servicio on premise o cómo configuras un servidor, pc o laptop y qué seguridad le pones, el antivirus, las exclusivas, etc.
Y, por último, de Accenture Security, cómo está posicionado en cuanto a los 4 grandes rasgos, que estamos considerados según Forrester, dentro de la categoría de los líderes y los strongers. Estamos muy bien posicionados junto con Deloitte y PwC, que son nuestra mayor competencia. Estamos líderes en el sector y en innovación y en nuevas soluciones.
Después del rollo de qué es Accenture Security, vamos un poco más en materia. Por ejemplo, qué entendemos o qué tiene que tener una gran empresa para estar segura o qué rasgos debe cumplir. Esta es nuestra idea, nuestro foco, pero hay que pensar que toda empresa necesita mayor o menor seguridad si… Hay que tener en cuenta que una PyME, su presupuesto para seguridad será mucho más pequeño que una gran empresa. Pero, también hay soluciones para esas empresas, no podemos dejar que solo una Accenture, un banco grande, tenga una protección bien hecha, sino que la PyME de una ferretería o una tienda de cualquier cosa, pues también tiene que cumplir ciertas normas y tiene que tener… No es tan atractivo para los hackers, pero siempre hay un nivel de riesgo.
¿Cómo vemos nosotros todo esto? Siempre hay un plan de contingencia o de gestión de la seguridad y después una estrategia de cómo abordar la seguridad, transformación al Cloud y unos riesgos. Cuando nos referimos a riesgos es que nosotros tenemos unos datos, por ejemplo, que son los que queremos proteger y qué riesgos hay asociados a esos datos. Es decir, yo tengo un banco, datos de cuentas bancarias, o de tarjetas de crédito, pues el riesgo es que yo tengo un asset, que son las tarjetas de crédito y qué riesgo hay de que estas me las roben, se exfiltren, etc. Dentro de esta premisa, vamos aplicando distintas capas. Ya veis que son las capas parecidas a los 3 grandes modelos que teníamos dentro de la compañía. Y sino, están englobados en todas.
Lo primero, tenemos data protection, todo el tema de cómo guardo los datos. Los tengo que guardar cifrados o no, es un dato crítico o no lo es. Si es crítico, lo guardo cifrado, cumpliendo con una encriptación concreta, etc. La parte de data lost prevention, que es el tema de filtrado de datos, en una compañía pensad que, en grandes compañías, si yo por ejemplo quiero exfiltrar información, eso puede estar controlado. Ejemplos que ha habido: se me viene a la mente, no sé si sois muy jóvenes, el caso de que Ferrari y Mercedes estuvieron, había un ingeniero de Ferrari que filtró los planos de los coches de F1 a Mercedes y lo pillaron, controlando sus correos, controlando su información y nosotros tenemos unas herramientas, llámese como quieran, que yo voy controlando un mail y si yo quiero enviar un mail con una tarjeta de crédito, un plano de un coche, o cualquier cosa confidencial, lo va a bloquear o lo va a dejar pasar pero me avisa. Y no solo el mail, sino lo copia en un pen drive o lo imprimo para llevarlo en mano.
En Application Security, todo lo que está relacionado a la seguridad de aplicación, aplicación web, un pase de datos, un servicio que nosotros por ejemplo tenemos publicado en Internet, hay que ponerle fronteras, como un wav, que es un firewall, que es un elemento que ponemos para proteger nuestros servicios. Si nosotros tenemos un servidor, no podemos publicarlo a Internet de cualquier forma, le ponemos un firewall delante, que lo que hará es bloquear o controlar todos los accesos a nuestro servidor. Pues un wav es un firewall que además está dirigido solo a aplicaciones web, porque tienen casuísticas especiales, es decir, un wav te protege de, no sé si os sonarán las siglas, de SQL inyection y otros tipos que son solo dirigidos para web.
¿Qué más tendremos? Pues la seguridad directamente de la aplicación con rusp o con romtime aplication security o firewalls solo para la aplicación, no genéricos, temas de protección del desktop o del laptop o de nuestra máquina, porque tan importante es proteger el servidor que nosotros ponemos de Internet del banco, como los PCs que están usando mis empleados. Porque igual tengo muy protegido mi data center o servidores con las tarjetas de crédito, pero tengo desprotegidos los equipos de los trabajadores y se pueden colar por un equipo de un trabajador. Le envío un email de phishing a un trabajador con un programa que se instala y tengo una puerta trasera abierta,

como el PC del empleado tiene acceso a todas las, a bastantes recursos del banco, por ejemplo, cuando ya se han colado, tienen acceso a todo lo del banco. Sin pasar por el otro lado, que era lo que estaba publicado em Internet que está más protegido.

Tema de Enterprise security pressions, pues todo el tema de monitorizar la actividad y monitorizar todas las herramientas que estamos usando. Podemos tener un firewall o distintas protecciones, pero por sí solas aportan valor, pero no el necesario. Yo puedo conseguir los datos si cojo los datos de un firewall, más los datos de un servidor, más los datos de otras herramientas, los puedo correlar y de allí puedo sacar que están, por ejemplo, intentando atacarme. El ejemplo más sencillo es el que llamamos de Superman, que es detectar que se están conectando a dos servicios desde dos países distintos. Yo estoy intentando entrar al servidor de España de una BBDD normal en España, pero mi usuario intenta también acceder a un servidor, pero esta vez desde Rusia y justo a la misma hora. Si los tenemos los blocks por separado del servidor, puede que no se vea este caso, pero si yo correlo los blocks de todos los servidores desde un punto central, que coge todos los blocks de todos los sistemas y los analiza, pues yo ya sé que están accediendo, que eso no puede ser, desde España y desde Rusia, a la misma hora y físicamente es imposible, con lo que una de las dos transacciones tiene que ser fraudulenta, estamos padeciendo u ataque.
Infraestructure Security, pues todo el tema de la plataforma y de la Red, todos los servidores sabéis que van conectados entre sí por swichers, routers o cualquier red, como tenemos en casa con el wifi o las protecciones que podemos tener con el wifi, pues podemos tenerlo en una empresa con el wifi también o en un data center como conectamos o interconectamos dos servidores, pues todas esas comunicaciones van o tienen que estar controladas. Controladas, cifradas, depende del caso.

Por último, os queda Cyber Identity, en Cyber tendremos 4 grandes bloques, como veis siempre hablamos de Threats, que son las amenazas, o qué podría pasar, si yo tengo una vulnerabilidad, tengo una amenaza de que me ataquen. Threat Response, cómo respondo cuando hay una amenaza o un ataque, lo que comentábamos de detectar los ataques, con un siem, por ejemplo, con el ejemplo de Superman, o detectar otro tipo de ataques de bots con otras herramientas. Threat Detection para detectar los ataques o vulnerabilidades, yo puedo analizar una máquina y puedo sacar todo el listado de vulnerabilidades o lo que queramos o, por ejemplo, hacer un pen test, que es lo más conocido, o lo que más atrae a la gente, que sería que yo ataco a una empresa, a un servidor, a lo que sea, yo contrato a una empresa para que lo ataque y me diga qué fallos de seguridad tiene y con este informe, siempre con permiso, yo puedo aplicar las medidas correctoras que sean necesarias. Hay gente que se dedica, entre nosotros, tenemos un pequeño grupo en España y uno muy grande a nivel mundial en Praga, que se dedica a esto, a atacar a empresas para detectar sus vulnerabilidades o si lo detecto yo la vulnerabilidad, pues la podré mitigar antes de que me lo pueda detectar un hacker o alguien o algún atacante malicioso.
Sí que hay que decir que eso siempre hay que hacerlo con consentimiento, al menos en nuestro país, porque la línea es muy fina, muchas veces no vale que tu ataque, porque tú lo estás probando en casa y ataques a una web de Zara o del Corte Inglés o de lo que sea, porque si no te han dado permiso… La línea es muy fina y la policía te viene a buscar, y conozco más de un caso.
Y en la parte de Identity, si quieres aportar algo Andrés…

AG: Aquí importante lo que comentaba Adri al principio, que todos estos grandes grupos, pueda aplicar en mayor medida a las empresas n función del tamaño y de la envergadura de la empresa, y lo que comentaba Adri era interesante, porque con empresas que son pequeñas, que puedes pensar que alguno de estos grupos puede no aplicar, tiene más importancia de lo que parece, y esta parte de Identity que es donde yo trabajo siempre, es un ejemplo, porque las identidades de los clientes que utilicen una plataforma web, para hacer compras que son comprar en un supermercado, quizá ahí pueda parecer que no hay datos

sensibles, no estamos hablando de un banco, no hay tarjetas de crédito, no hay dinero de por medio, pero solo con que consigan las credenciales de un usuario que accede, pueden ir pivotando en aquellos servicios, webs, donde ese usuario tenga el mismo correo electrónico y probar a ver si es uno de tantos que utiliza la misma contraseña en todos los sitios, entonces al acceder a una plataforma aparentemente sin riesgo, que está poco protegida por la compañía, consigues llegar a otros sitios más lejanos, que a pesar de estar mejor protegidos, al tener las credenciales poco vas a poder hacer.

Entonces, aquí lo que comentábamos, que tenemos como pilares fundamentales, sobre todo lo que da nombre al grupo, que es Identity management y Access management, lo comentaremos en detalle después. Identity Management sería la gestión de identidades. Access management sería la gestión de accesos. Directory Services, sería todos aquellos repositorios donde se almacenan las identidades, y luego el informe de autorización y autenticación, para ver en qué punto de la infraestructura forzar a que una determinada transacción tenga que ser autenticada y, además, autorizada. Y aquí no entro más en detalle, porque lo vamos a explicar más adelante.

AC: Ahora entraremos más en detalle en la parte de Cyber, y posteriormente en la de Digital Identity. ¿Cuáles son los cuatro pilares o las cuatro premisas que tenemos dentro de Cyber? Pues la identificación de todos esos threats, vulnerabilidades, la protección, la detección y el response and recovery. En todo identificar siguiendo esos pasos cuando empezamos desde cero, siempre tenemos que ponernos o usar herramientas para identificar. Identificar vulnerabilidades las puedo identificar en test, como os comentaba, o podemos usar herramientas que detecten vulnerabilidades, como qualys, nesus, sisdic, etc. Que escanean nuestros servidores, nuestra Red y nos dicen pues: eres vulnerable a tal cosa, a tal cv, como llamamos a las vulnerabilidades. Todas tienen un código, que es un cv.

Una vez detectadas esas vulnerabilidades, podemos hacer un informe y pasar a la protección. ¿Cómo podemos proteger? Pues podemos proteger con medidas de aplicar medidas de corrección. Por ejemplo, si me ha salido una vulnerabilidad en JAVA, o Windows, igual es simplemente que tengo que actualizar la máquina a una versión más nueva por el parche de seguridad.

¿Qué políticas tiene una empresa de patch management o actualizaciones? Para que siempre tengamos el sistema lo más parcheado posible.
Pensad que la premisa de seguridad más importante siempre es tener los sistemas lo más actualizados posibles. Y esto es una cosa que no se cumple muchas veces, nos hemos encontrado en muchas empresas, que igual tienen servidores que igual usan Windows Server 2003 o Windows XP, totalmente descatalogados, pero que por su aplicación no pueden usar otra cosa, pues tendremos que meter medidas compensatorias para detectar esas partes.
Una vez tenemos protegido o los puntos que queramos, actualizaciones, por ejemplo, no exponer los servidores a Internet directamente, controlar a los usuarios que acceden, ligado a la parte de Andrés. Yo a un servidor expuesto, no puede acceder cualquiera, no solo que no puede acceder cualquiera, sino que incluso cada usuario que accede necesita tener un rol especial. Es decir, que no todos los usuarios que acceden a un servidor web que tenga expuesto a Internet, debe tener permisos de administrador.
Entonces, hay una serie de premisas o de protecciones que hay que cumplir, y después pasamos a la detección, que no solo es esto, sino que hay ataques de día 0, hay ataques de otro tipo de ataques, que por muchas protecciones que pongamos, por muchas actualizaciones que tengamos, hay que descubrirlas, o hay que detectarlos. Aquí usamos herramientas, como los IDS o IPS, que son, o los firewalls, que son herramientas que detectan mirando patrones, mirando tipos de tráfico, pueden llegar a detectar que me están haciendo este ataque. Me están intentando hacer este ataque. Me están intentando hacer un ataque de fuerza bruta, que es que un usuario y una contraseña, intentan probar todas

las combinaciones hasta que encuentran la que es correcta. Como más difícil sea la contraseña, o más larga sea, pues un ataque de fuerza bruta, más tiempo costará de detectar o de que sea válido, y si podemos poner otras medidas de protección, como, por ejemplo, en el móvil, que intento desbloquearlo 5 veces y se me bloquea 30 segundos, o un minuto. Pues lo mismo lo podemos hacer en servidores. Y seguramente en algún caso lo habréis encontrado, y así mitigo los ataques de fuerza bruta y los detecto porque estoy viendo que hay intentos fallidos de log in o de acceso, en un minuto hay 300, pues ahí está pasando algo.
Una vez hemos detectado, ¿cómo respondemos y cómo nos recuperamos? Pues si es un ataque de estos, bloqueo la IP que está intentando acceder a ese log in, y si yo la bloqueo con el firewall, no la permito que pase, el ataque lo hemos parado. Ese es un ataque sencillo, pero ¿qué pasa cuando son ataques más complicados o son ataques que no nos enteramos? Aquí entra el tema del forense. Una vez hemos descubierto que tenemos un ataque, hemos de descubrir cómo tiramos atrás y vamos descubriendo las vulnerabilidades o por dónde han entrado.

Tan importante es parar un ataque, como recuperarnos o saber de dónde ha venido. A veces hay ataques que no podemos parar, hasta que detectemos por dónde ha venido o cómo ha entrado. Porque si solo nos dedicamos a parar el ataque y mitigarlo, puede que, en un cierto tiempo, si no hemos corregido los errores que tenemos, se nos colarán por el mismo sitio.
Si el ataque ha sido un ram somewhere, que no sé si os suena, es un malware, un virus, que nos cifra todos los datos de un ordenador. Nos puede cifrar todos los datos de nuestro PC, como puede cifrarnos todos los servidores o todas las BBDD y todos los… y después nos piden un rescate. Pues tan importante es recuperarnos y recuperar los datos como saber por dónde ha entrado. Si ha llegado por un mail o cómo ha llegado a ejecutarse o a entrar en la compañía. Si ha llegado por un mail podemos hacer campañas de concienciación, hacer o bloquear ciertos tipos de archivos, etc. Si ha entrado de esta manera, pues bloqueamos para que no nos vuelva a pasar.
Después tenemos las defensas activas que son el último punto, la evolución más madura de la ciberseguridad, que es usar herramientas que ataquen o simulen ataques para ver cómo tenemos la plataforma de estable y cómo podemos proteger.
Veis que todas las distintas opciones o distintas fases, de la protección, van muy interconectadas entre ellas. Yo, desde el vulnerability management, que es la detección de las vulnerabilidades, el reporting… el alimento al Threat hunting, que será la colección de datos de vulnerabilidades, para nosotros y para terceros. Pensad que en Threat hunting, lo típico es interconectarse o compartir información con todas las compañías, grandes compañías como un Palo Alto u otras que dan servicios como firewalls, lo que tienen es BBDD muy grandes de si he detectado un ataque o un fichero malicioso en tu organización, eso lo publico en mis redes para que las otras compañías que están usando mis servicios sepan que ese fichero es malicioso. Por ejemplo, detectamos un ataque de día 0, que es ese ataque que no se ha detectado nunca antes, es la primera vez que se detecta, y lo detectamos en Accenture. Pues, si lo detecta un firewall Palo Alto o cualquier herramienta, él publica en sus servicios para que los bancos que están usando Palo Alto también, se le actualicen las BBDD y así están todos protegidos a ese 0 Day. Y así, todos estamos protegidos. Yo, una vez ayudo a los demás, y los demás me ayudan a mí. Es un poco como una comunidad.

Y veis que todos están intercomunicados y todos van relacionados. Uno no existe sin los otros. Ejemplos de herramientas que podemos usar en cada uno de los apartados, lo que os he comentado al principio. De vulnerabilidades los más famosos son Qualys y Nexus Teneble, en Threats podemos tener Titanium etc, para Esiem, splunk, servicios de Palo Alto, para data prevention, el más típico Symantec, junto al de Microsoft. Y veis que cyber va cogiendo también, interconecta todos los puntos que teníamos antes. Todo el data lost prevention, que era del apartado de data protection, y los estamos viendo en cyber, porque necesitamos los datos de data lost prevention para gestionarlo. El end point protection, es del tema de protección de infraestructura, pero lo vemos aquí también.

Y, por último, de la parte de Cyber, que no quiero meteros demasiado la chapa, ¿cómo empezaríamos? ¿Cuándo tenemos una empresa por dónde empezamos? Pues estos son los pasos. Empezaríamos por Threat prevention, aplicar herramientas, es decir, un firewall, un IDS, un IPS, una protección. El siguiente paso, para ser maduro, vulnerability management, aplicar Qualys o Nexus para detectar nuestras vulnerabilidades y corregirlas. El siguiente es el siem, es la herramienta para gestionar o correlar todos los servidores, de todas las herramientas. Siguiente el operation monitoring, que es un shock, que es una plataforma donde hay gente monitorizando y viendo en tiempo real, todo lo que está pasando en nuestra empresa, para si hay un ataque, lo podamos detectar al momento, o con la medida más rápida posible. Seguiríamos por Threat Intelligence, Threat active deffense. Pesad que los 4 primeros puntos, hay muchas empresas que ya lo tienen, y lo que estamos moviendo ahora más, son los 3 últimos, es lo que está más de moda o lo que intentamos aplicar o aportar a los clientes. Porque ya se lleva años con el tema de seguridad, y con el tema de ciberseguridad, con lo que los primeros puntos ya están aplicados, y vamos un punto más allá con los 3 puntos siguientes.
La parte de digital, Andrés, todo tuyo.

AG: muy bien. Pues para comenzar con esta parte, era importante que todo el mundo tuviese la foto clara, por eso hemos cogido directamente la definición de digital Identity, que no es más que toda la información relacionada con una entidad, que puede ser una persona física, organización, aplicación o un dispositivo. Todos esos atributos conforman una identidad digital, que van a utilizar distintos componentes, distintos servicios a lo largo de una compañía. Entonces, al final es, nuestra propia referencia en Internet o en Intranet en caso de la empresa. Y es en torno a lo que gira todo lo que hay en el grupo en el que yo trabajo, en digital Identity. Con esto en mente, en la siguiente slide, comentábamos antes que los dos pilares fundamentales eran Identity management y access management. Tiene que haber una conjunción de ambas y lo que nos habíamos dejado pendiente es cuál es la diferencia. Entonces, Identity management es la gestión de identidades, es traer u ofrecer estas identidades digitales a aquellos lugares en los que se necesiten, a lo largo de los distintos sistemas de la compañía, y además, cuidarlas, tener cuidado de ellas y tenerlas siempre al lío, siempre cuidadas y sincronizadas a lo largo de todo el tiempo que esas identidades permanezcan vigentes.
Y el access management es darle a un usuario, un ID exclusivamente con los permisos que necesita. Uno es controlar la identidad como algo tangible y access management, es controlar a dónde está accediendo cada persona. El objetivo común de los grupos de ciberseguridad es minimizar riesgos. Todo unido con una capa de gobierno que lo mantiene sincronizado.
Esto es una base, ahora lo veremos en detalle. En la siguiente slide, tenemos cómo ha ido evolucionando lo referido a identidad digital a lo largo de la historia. Todo comenzó intentando poner contraseñas a todo y poco a poco intentar complicarlas. Primero contraseñas básicas, luego con números y letras, luego números y letras, mayúscula y minúscula. Mucha gente no entendía esto o no seguía esto, y al final la gente intentaba hacer contraseñas tan difíciles que al final eran difíciles de recordar y lo escribían en una nota. No sería la primera vez que vamos a un cliente y tienen las contraseñas tiradas por la mesa y a lo mejor son contraseñas para entrar a una BBDD de clientes de la compañía.

Además, esto tenía dos puntos negativos. El primero era que por mucho que uno piense que le cuesta recordar su contraseña o credenciales, para un sistema automatizado puede ser muy sencillo averiguarlas con ataques de fuerza bruta que comentaba Adri al principio. Y además, cuanto más la compliques, más vectores de entrada abrirás, porque habrá más gente que no se acuerde de su contraseña después de mucho tiempo sin utilizarla. Más gente habrá que intente reestablecerla, y aquí tenemos un vector claro. El cómo se gestiona reestablecer la contraseña. Esto está ligado con Identity management, cómo se reestablecen las credenciales de los usuarios, se les envía un mail, cómo te aseguras de que la dirección es la correcta, cuánto tiempo de caducidad tienen los enlaces… Son cosas que nos encontramos en

el día a día, por eso esta parte la gente la suele ver muy reflejada en su día a día. Además, aquí se lleva un control de histórico de contraseñas para que no puedas repetirlas. Muchos vectores que hacen que sea más fácil el ataque.

Y, en la siguiente slide, al final es el resumen, que es que nada es seguro, es decir, no te fías de nada, no te vale ni una contraseña simple ni una compleja. Todo tiene su contra y al final hay que darle una vuelta, hay que inventar nuevas formas de proteger las identidades digitales, que es lo que intentamos siempre.
En la siguiente slide, lo que tenemos es el primer pilar fundamental, que hemos dicho que era Identity management. Aquí arriba, podéis ver algunos partners de Accenture, pues empresas como SailPoint, proveedores de servicios como incluso IBM, y hemos dicho que se basaba en la gestión de las identidades a lo largo de los sistemas de una organización. Tenemos que pensar que hay diferentes tipos de identidades. En una empresa, según el tipo que sea, puede haber identidades de clientes, de empleados o incluso identidades de partners, de otras empresas que son clientes, pero tienen ciertos privilegios como empleados en según qué zonas.
Estas identidades se tienen que provisionar donde se necesiten, se pueden almacenar en repositorios, que pueden ser estándar o no tanto, las identidades pueden estar en los mismos repositorios o distintos, y a la hora de provisionarlas podemos tener aplicaciones que sean compatibles con estos repositorios estándar, como la de Microsoft… al final es el estándar más básico para el almacenamiento de identidades, y otras aplicaciones que de forma nativa no se puedan integrar y haya que adaptarlo.
Hemos dicho también que era importante llevar un cuidado, un mantenimiento de esas identidades a lo largo del tiempo, porque tienes que llevar cuidado de revocar las identidades cuando el usuario deja la compañía o deja el área o proyecto, tienes que mover la identidad de sitio… y migrar las identidades de antiguos repositorios. Hay muchos proyectos de Identity management que van ligados a mover las identidades a repositorios estandarizados o más modernos que ofrezcan posibilidades que los antiguos no, que suele ser complejo. Tenemos que pensar que un repositorio de identidades es provisionar las identidades a distintos componentes, estos componentes ya están integrados con sistemas de almacenamiento de identidades y no es sencillo, no es desconectar un cable y conectarlo aquí.
Además, relacionado con la consistencia de las identidades, tenemos la sincronización de cuentas porque puede ser que las identidades estén en distintos repositorios, e incluso capacidades de autoservicio. Cómo un sistema es capaz de ofrecerá un cliente o u usuario, que no tiene por qué ser un cliente, la posibilidad de él mismo manejar sus propios atributos, su propia cuenta, tanto como sea posible, sin que eso suponga un riesgo de seguridad.
En la siguiente slide, tenemos el siguiente pilar, que es el access management, que se basa en la gestión de accesos de usuarios, a los sistemas de una compañía. Uno de los partners más importantes que trabajan con Accenture es Forgerock, aunque trabajamos con muchos otros. Esto si que es visible realmente porque todos lo vemos a diario. Para la gestión de accesos de usuarios, siempre todo va dividido en fases. La primera siempre será autenticación, que es la fase por definición en la que se verifica que un usuario es quien dice ser. Aquí, va ligado con la red que comentábamos antes. Todo comenzó con autenticación simple, pero va a evolucionando, a autenticación lo más compleja, pero user friendly que se pueda, añadiendo biometría, añadiendo autenticación multifactorial, con envío de one time password al móvil, notificación push o al correo o incluso combinar las fases de autenticación con los mecanismos con detección de coacción. En según qué países puede ser más útil que en otros.
Aquí siempre que tenemos que tener algo claro y es que afecta al usuario final. Si un cliente o usuario, piensa que una aplicación es compleja de utilizar, por mucho que le digas que es segura, le importa, pero le importa menos, le importa más que una aplicación sea fácil de utilizar. Si pones muchas trabas para entrar en tu cuenta bancaria, lo más seguro es que dures un mes y te busques otro. Hay muchas ofertas y no te vas a quedar con la peor aplicación. Entonces, eso siempre hay que tenerlo en cuenta a la hora de manejar la experiencia de usuario y el resumen es elaborar el mecanismo de productos de autenticación seguro pero sencillo de utilizar.

Después de la autenticación viene la autorización. Una vez se ha autenticado, ya está dentro y está identificado con una sesión abierta, hay que manejar la autorización, hay que saber medir a qué recursos tiene acceso ese usuario. Entonces, siempre tiene que estar autenticado y aquí es donde se aplican niveles de autorización distintos, de grano fino o grano grueso, en función de cuántos o cómo de complejo sea el entramado de autorización que quieras aplicar o distintos tipos de políticas. Incluso tenemos la gestión del consentimiento, que es algo nuevo que comentaremos después. A este respecto, pues siempre tener claro también que todo de ir desplegado como decía Adri, en plataformas lo mas modernas posibles, entornos cloud, DevOps e irnos alejando de los entornos on premise que conocíamos hasta ahora, y aquí es muy importante el tema de la estandarización, que va ligado con una pregunta que hacíais, porque al final todo tiene que seguir unos estándares. Cada empresa nova inventarse una forma de autenticar distinta. Se definen unos estándares para todos en los que basar ciertas comunicaciones. Las comunicaciones de autorización se basan… es la definición de un estándar en el que basar los mecanismos de autenticación y autorización que implantas en una empresa.
Y, por último, tenemos en la slide siguiente un tercer pilar que se conoce como PAM. El primero era IPM, el segundo AM y este es PAM, que es priviledge access management. Es muy importante porque aquí no hablamos de la protección de las cuentas, aquí hablamos con cuentas con privilegios de administración de sistemas, ya no son tampoco en datos de usuario, que puede serlo, sino cuentas de servicio, cuentas que utiliza un software, una cuenta que utiliza un componente tecnológico, que por un motivo o por otro, tiene privilegios de administración, necesita acceder a sistemas con ciertos privilegios, por ejemplo, para monitorizar. El uso de estas credenciales tiene que cuidarse mucho más porque el hecho de que se exfiltre una identidad de este tipo, una de estas cuentas, puede comprometer toda la compañía entera.
Comentaba con Adria también, que es por poner un poco el símil, no es lo mismo que alguien robe la llave de una puerta de una casa de 50 plantas que alguien robe la llave donde está el cajetín con todas las llaves de todas las puertas. Esto es más o menos lo mismo. No es donde residen las identidades sino cómo se están utilizando y para lo que son críticas. Lo que se suele hacer siempre es asegurar que se monitorizan todas las sesiones de administradores con acción de vídeo y comando para ver que están haciendo, sobre todo a la hora de analizar un incidente, aplicar siempre contraseñas robustas para estas cuentas y almacenar las cuentas no solo credenciales, sino algunos secrets, algunas claves o certificados, de forma segura.
Ahora os vamos a contar algunas anécdotas que tenemos sobre proyectos en los que hemos participado.

AC: Sí, queremos contaros un poco casos de éxito que hemos tenido con clientes, o más o menos para que os hagáis la idea de qué hacemos en el día a día con nuestros clientes. Casos reales de clientes con los que hemos trabajado.
Yo he estado trabajando en varios clientes, con tema de cabernets y del entorno de containers, que para quien no lo sepa, es el nuevo paradigma o la nueva configuración que se va a usar ahora para el tema de servicios o servidores. Empezamos con servidores físicos donde cada servidor tenía un servicio, como una web, y necesitabas tantos servidores como webs querías exponer, que eso era muy difícil de escalar. Pasamos a máquinas virtuales, donde en un servidor físico, tenías varias máquinas virtuales, tener varios servidores con BBDD o con webs o con cualquier servicio que se nos ocurra, en un mismo servidor físico. ¿Y cuál es el tercer paradigma? Es pasarnos a un entorno de containers. Container es un servicio pequeño, solo la web, solo la BBDD, una acción, que se ejecuta en un container o en un Bot de entorno OpenShift y que es fácilmente escalable. La idea de los containers es que yo puedo tener una imagen base con una web, que es fácilmente escalable, y en la plataforma si tengo un Black Friday o una subida en rebajas, cualquier cosa, por ejemplo, yo puedo escalar muy fácilmente dentro de la plataforma y crear tantos bots como necesite para dar abasto a nuestros clientes.
Dos mundos nuevos que estamos ahora en auge son el mundo Cloud y el mundo containers. Entonces, hay dos maneras de aplicar seguridad, nuevas maneras de aplicar

seguridad, en esos dos entornos. También hay la combinación de los containers y mundo Cloud. Todos los proveedores Cloud, tanto Amazon como Azure como Google, te ofrecen entornos cabernets, donde puedes subir los containers. De containers nos referimos a cabernets y OpenShift, que es la versión de RedHat de pago. Es el más conocido por ser el Open Source.
Y qué tenemos. Pues tenemos vectores de ataque nuevos. Aquí hay que proteger desde Cyber o desde Protection, vemos estos nuevos vectores de ataque y cómo los protegemos.
Pasa que tenemos en containers security, tres capas a proteger. Foundation, que sería la protección del entorno físico donde se desplegará la plataforma, la parte de la plataforma, que es el Docker, el OpenShift, el cubernets, que cada uno tiene sus configuraciones de seguridad, tiene sus restricciones que podemos configurar o modificar. El tema de donde se almacenan las imágenes del container. Si alguien la ataque y consigue meter una imagen vulnerable, cuando la ejecute en la plataforma, esa imagen se levanta o se ejecutará con una vulnerabilidad o con un ataque o cualquier cosa.

Y el pass overlay, es la parte del container en sí, el Bot, es decir, qué vulnerabilidades o cómo protejo el container en sí, que puede ser web con un JAVA corriendo, es vulnerable porque usan un JAVA 6, como puede ser un apache que está usando una versión antigua, como puede ser cualquier cosa. Y de aquí podemos meter protecciones como el rusp, que es un firewall, que se ejecuta o protege el Bot. El wav antes, teníamos delante para proteger las aplicaciones web, ahora tenemos un firewall más dentro, solo protegiendo ese container en concreto. Cualquier duda, después lo explicamos.
Pasamos un poco rápido que nos quedamos sin tiempo.
¿Qué tenemos en cuenta en un entorno de containers? Todas estas capabilities o funcionalidades que deberíamos estar controlando. No todas son de Cyber, por ejemplo, temas de CI, CDI, es parte de Application, otros temas de Cyber como el escaneado de vulnerabilidades… Pero hay temas de red o de forense que son de otras ramas, o tienes el tema del R Back que es de digital, porque tienes que definir los roles que necesitas… No solo las identidades que van a acceder a tu plataforma, sino qué permisos tienen. No es lo mismo que todos los administradores de los cubernets tengan permisos de administrador. Pues definiremos un R Back, que será qué usuario, qué permiso tiene. Crearemos 4 roles, 1 que solo pueda leer, 1 que solo pueda editar tal cosa porque es lo que necesita, otro con administrador… Pero controlaremos mucho qué hacen.
Ejemplos, o cómo nosotros podemos mitigar los riesgos. Tenemos una serie de riesgos, como exploids, ataques de navegación de servicio, security compromised, o containers que se rompen, etc. Que se pueden proteger con distintas herramientas que lo que se encargan es de escanear en búsqueda de vulnerabilidades o proteger a tiempo real. Splunk para el tema de Threat Intelligence y siem, la registries, que es donde se guarda la imagen, pero es importante que donde se guardan las imágenes para los containers estén correctamente securizadas. No es lo mismo que cualquiera pueda subir una imagen o que solo quien yo diga pueda subir una imagen o modificar. Cyberark para las identidades, Blackduck para escanear y ver el código y Splunk otra vez para siem.
Pensad que también, en el nuevo paradigma de containers, entra en juego el DevSecOps. Hay el DevOps y el DevSecOps. DevOps sería que yo estoy desarrollando, por ejemplo, JAVA, y usando Jenkins u otras plataformas, lo despliego y lo puedo ejecutar en un container y probarlo, pero ese código, que he creado un JAVA, ¿cómo es de seguro? Puedo poner herramientas en medio, que sría el DevSecOps, que si estoy programando en JAVA u otro, antes de que eso se publique a producción o a test o lo que sea, pasa unos ciertos controles y tengo una herramienta que lo que hará es escanear si el código tiene vulnerabilidades, si hay cosas mal, o puede ser un Sonar Qeue u otras herramientas y vamos analizando el código para que cuando llegue la imagen a estar ejecutándose en mis servidores, esté lo más segura posible. El DevSecOps lo lleva el equipo de Application Security. Y de la parte de Digital…

AG: Aquí hemos participado también en la creación de un banco desde cero, que es a lo que hace referencia este ejemplo, montando una arquitectura escalable de autenticación y autorización para que como hemos dicho, y aquí en un entorno bancario, hace referencia a la gestión de identidades y accesos, cómo se guardan, tratan, cómo y cuándo se dan de baja, con qué componentes se integran, sobre todo de monitorización de acceso para futuros bloqueos, posición de riesgo, exfiltraciones de datos… para la parte de gestión de accesos, determinar qué puede hacer el usuario cuando accede, desde dónde accede , cómo se autentica, cuál es el flujo de autenticación según si accede desde el móvil, la aplicación web del banco, desde un cajero, banca telefónica y también para los empleados, cómo acceden a las aplicaciones desde la intranet para gestionar las consultas de los clientes cuando están en la oficina.
Aquí hay una parte interesante, que es Netflix, que estaréis pensando qué pinta Netflix con el banco, y es que a pesar de que todo el mundo lo conozca por ser el principal proveedor de streaming en el mundo, son pioneros en el desarrollo de software, de componentes, que más tarde libera y están tan bien hechos, que el resto de empresas lo reutilizan, liberan parte de su código para que todo el mundo lo pueda utilizar y estas empresas lo reutilizan. En este caso fue el api que desarrolló Netflix, que se llamaba Soul y se utilizó para esta implantación.
Una de las preguntas que hacía una de las personas que está en la reunión, que era cómo se almacenan las identidades, que luego respondes.
Tenemos también otro caso que fue muy interesante por el hecho de ser el desarrollo de una plataforma bancaria desde cero, nosotros participando en la parte que nos tocaba, de gestión de identidades y control de accesos, fue para una plataforma bancaria a nivel mundial, cómo crear un control de autenticaciones de todo el mundo desde distintas regiones. Una de las cosas más interesantes, aparte de lo que hemos comentado a nivel técnico, es tener en cuenta cómo aplican las legislaciones, porque no es lo mismo los usuarios que acceden desde China o desde Rusia, que tienen legislaciones muy estrictas, que determinan que las identidades no pueden salir de Rusia y China. ¿Cómo haces eso intentando desarrollar un Hub mundial para encauzar todas las autenticaciones de los usuarios de una plataforma bancaria en distintas partes del mundo? Muy interesante también.
Tenemos algo mencionado antes en las dos siguientes slides, que era que seguramente a más de uno nos ha llegado en los últimos meses un mensaje de nuestro banco, diciéndonos que debido a la nueva legislación hay que dar un consentimiento para tal cosa, que solemos leer, aceptar y fuera. Todo esto va relacionado con una directiva que se creó en el marco europeo, que se llama PSD2, que es una directiva de servicios de pago, para regular el acceso de terceros a las apis de los bancos. A día de hoy, si saliera una aplicación que te puedes bajar en tu móvil y te sirve para gestionar cuánto estás gastando en tus tres bancos de los que eres cliente, le tienes que dar tus credenciales, que la app, vaya a los tres bancos y autentique, baje lo que ve en pantalla y lo muestre de esta forma. Esto vale una vez, pero cuando se hace tenso, hay que regularlo, no puedes dar tus credenciales, así como así.
Entonces, todos los bancos que han ido abriendo sus apis y han donado las arquitecturas a estos terceros y a la vez al resto de bancos, pproque son terceros de los demás. BBVA es third partie de banco Sabadell y este es third partie de BBVA.
Para todo esto, se definen una serie de artículos, de seguridad, gestión y cómo se maneja el tema, todo basado en el consentimiento del usuario, que tiene que durar 90 días, y con el consentimiento el usuario decide a qué partes del banco, de sus cuentas y sus balances y gastos, le da acceso a este tercero. Entonces, que sepáis que estos mensajes se basaban en esta directiva y una cosa en la que nosotros hemos estado trabajando es un estándar llamado UMA, que precisamente sirve y se puede aplicar para este tipo de cosas, como vemos en la última slide, la siguiente, que es cómo esto funciona a nivel técnico.
Aquí, un ejemplo sencillo, es… no en el entorno bancario porque se puede aplicar en cualquier sitio, pero el tema de consentimiento funciona muy bien en el entorno médico. En este caso, un paciente al final es lo que aparece abajo, el Resource Owner, el dueño del recurso, y el recurso es su historial médico, que se almacena en un servidor donde se almacenan todos los

historiales médicos, el suyo en este caso.

Protege este recurso, este esquema está sacado de la documentación pública de Forgerock, uno de los partner de Accenture y de los pioneros en UMA.
El usuario, que al final es dueño de su propio historial médico, controla este recurso a través del athoritation server y una request impact, que es el médico, accede al cliente, el cliente hablando siempre de un componente técnico, puede ser el PC de su consulta, accede aquí y necesita autorización que se maneja en el authoritation server, para poder acceder al historial médico de la paciente o el paciente.
Esto es el concepto y se aplica, va relacionado con el consentimiento, con lo que aplica muy bien a la parte de PSD2, y cómo se han diseñado arquitecturas en las que hemos participado para cubrir todo lo que la directiva ponía como necesidad. Porque al final era que o los bancos se adaptaban o les seguían haciendo web scrabing, pero nadie quiere eso porque implica riesgos de privacidad, como que le tengas que dar tus credenciales a un tercero y no te fías de cómo las trata. Y ahora todo está estandarizado, como poco el proceso en función de cómo de avanzada esté cada entidad bancaria en el cumplimiento de la directiva, y cada tercero. Porque luego la empresa que es third partie, se tiene que adaptar a esto y es uno de los objetivos, no solo regularizar y proteger sino también que aumente la oferta de funcionalidades como aplicaciones de agregación bancaria para controlar tus gastos a modo global u otras cosas que puedan salir en el futuro.
Y creo que…

BE: creo que sí, vamos a pasar al turno de preguntas, ha habido alguna pregunta durante la presentación. Empezamos por la primera, Carlos García dice: buenos días, dado que ha aumentado el teletrabajo durante la pandemia, cuál es el mayor riesgo en los entornos corporativos que habéis detectado por este motivo.

AG: Realmente, depende del entorno, pero las dos cosas que en nuestro ámbito hemos visto, Adri tendrá otras, por un lado, son las VPN, porque todo el mundo que intenta acceder a los sistemas de su empresa trabaja desde la oficina porque tienen una intranet para no tener que abrir sus sistemas a Internet. El problema se plantea en cómo acceder desde casa. Se monta un VPN en realidades virtuales, que no están correctamente securizadas y abren un montón de amenazas para poder atacar una empresa desde el PC del empleado que esté intentando acceder.
Por otro lado, algo que no sería unataque pero que es fastidioso, es la abnegación de servicio, que provoca el aumento de gente que está conectada con VPN, porque muchas no están dimensionadas correctamente porque no pueden acceder todos los empleados desde una VPN, y si cae por exceso de carga, nadie puede acceder.
Esas son de las más típicas y son lógicas por la situación actual.

AC: en el caso de Cyber, lo que más hemos encontrado es la aparición de nuevos tipos de ataque, aprovechando la casuística del Covid, los que ya se dicen por la, o se comentan por la tele de que un nuevo ram somewhere, que aprovechando la temática del Covid y los temas de Phising, con el Covid, aparte de que es más complicado cuando tienes el PC en casa, monitorizar a los teletrabajadores, sus sistemas, monitorizar en el sentido de que el antivirus tenga todas las actualizaciones, eso está preparado para que normalmente lo tengas desde la empresa, y si lo tienes desde casa igual no puedes conectarte para decirle al servidor que estoy actualizado y lo tengo todo bien o simplemente que se te descargue el paquete de virus nuevos o etc.

BE: Jessica Rubio pregunta: ¿cómo sabéis al iniciar un proyecto, qué tipo de seguridad debe instaurarse? ¿qué tipo de estudio debe realizarse?

AC: Pues a priori no lo sabes, sí que hay proyectos que lo que te piden es algo muy concreto y entonces vas a eso y ya está. Si no lo que tienes que hacer es un estudio. Empiezas con un estudio de riesgos y lo que tienes que detectar es tus puntos flacos y tus riesgos, tus assets asociados a esos riesgos. Me explico, yo tengo una serie de assets, como mis tarjetas de crédito que uso para el banco, y eso es lo que tengo que proteger. Eso es un asset. Y qué riesgos tengo asociados. Según eso, vas

construyendo las otras capas de arquitectura para proteger eso. Y también es importante determinar el riesgo que hay asociado a un asset, porque si no voy a gastarme un millón de euros en proteger un asset, que si lo pierdo me cuesta 100.000 euros. Es importante saber ese asset, para la compañía, qué dinero le puede costar si me lo roban o me lo exfiltran o cualquier cosa. Porque no me voy a gastar más dinero en protegerlo de lo que me cuesta.

AG: es interesante saber que cada cliente es un mundo y depende de lo que necesito. Tú necesitarás implantar una serie de sistemas, más una serie de protecciones u otras. Lo primero es analizar lo que comentaba Adri, riesgos y sistemas que está ofreciendo. Todo tiende a estandarizarse. Todas las arquitecturas suelen tener distintos proveedores, pero todos deberían tener unas herramientas parecidas. Sabes cuál es la estructura base y la que tú deberías recomendar para que todo esté estructurado de una forma lógica, para prevenir riesgos que se puedan prevenir directamente montando algo que es lo que suele montar todo el mundo.

AC: También tenemos muy claro, muy diferenciado el tipo de empresa que es, si es una empresa que se dedica, una financiera o un banco, o es un retail, products… a qué se dedica. No es lo mismo proteger los riesgos de un banco que los que tenga una tienda online o un Endesa.

AG: no es lo mismo tampoco la protección de vulnerabilidades que proyectos en los que participamos en el despliegue de todos los componentes. Siempre hay distintas formas de abordarlo.

BE: Marta Lechuga pregunta: ¿os habéis encontrado en alguna ocasión con que han atacado a un cliente y no habéis descubierto cómo le han atacado y por dónde han entrado? ¿qué se hace en esos casos?

AC: de momento, no. Pero sí que te puede costar más o menos, sí que puede haber investigaciones que duren meses y que tardes meses. Normalmente acabas encontrando por dónde ha entrado. Pero si que puede ser largo, porque las evidencias se van volatilizando y hay evidencias que es complicado obtenerlas, porque si las tienes en tu memoria RAM en el PC, solo que apagues el PC, esa evidencia se va.

AG: Claro, está muy ligado con cuántas evidencias tienes. Esa pregunta va muy ligada con cuánto tiempo tardas en encontrar el vector de entrada. Si no lo encontrase o tardo mucho es porque hay gran cantidad de información o porque no todos los sistemas están debidamente monitorizados. Y si fuese el caso de que no llegas a detectar con evidencia, haciendo forense, la entrada, el vector de entrada, lo que tienes que hacer es un análisis de riesgos de todos los componentes y donde sepas que hay un riesgo, sepas o no si ha sido explotado, directamente tapar agujeros. Si no has sido capaz de detectar el vector de entrada, pero sabes que tienes 20 candidatos, lo tienes que cerrar.

BE: Josema Vizcaíno pregunta: ¿qué se refiere con directorio de identidades?

AG: Aquí hablábamos de dónde reside la identidad de usuario. Como usuario de Amazon, tu identidad está dentro de un componente que hay dentro de Amazon y todos tus datos, usuario, contraseña, nombre real, email, dirección… Se almacena en repositorios que suelen ser estándar. Suelen ser directorios activos de Microsoft cuando entras en tu PC, está almacenado en el directorio activo de tu PC, o si hablamos de una compañía en el directorio activo de tu compañía, o en LDub que es el directorio por excelencia de almacenamiento de identidades u otros estándares distintos. Al final es dónde reside finalmente tu identidad, todos tus datos.

BE: Alfonso pregunta: ¿qué responsabilidad final tenéis con el cliente que habiendo implantado vuestros protocolos de seguridad ha recibido ataques con éxito?

AG: esta pregunta es interesante y está relacionada con la siguiente que hace referencia de Nacho, al final todo lo que hacemos nosotros en compromiso con el cliente, es siempre dar las mejores recomendaciones y llevar a cabo los proyectos de la forma más segura posible, pero muchas veces las recomendaciones se quedan

ahí, en recomendaciones. Entonces, un cliente final cuando sufre un ataque y al final se pone en riesgo la identidad de los clientes de un supermercado, el supermercado será el primer responsable y podrá delegar o no, algún tipo de responsabilidad en función del tipo de acuerdo que tenga con sus proveedores, pero lo que nunca va a poder eludir, será la responsabilidad que como entidad tiene con el cliente. Todo depende siempre del contrato y lo más importante es que nunca una compañía puede evadir ningún problema de este tipo que tenga, porque la responsabilidad con el cliente es suya. No solo eso, sino que muchas veces se hace un set de recomendaciones de que esto se debería de montar así, pero la última palabra la va a tener el cliente. Al final nunca vas a tener la responsabilidad de que tus recomendaciones se hayan seguido o no.

AC: También hay que tener en cuenta que no hay sistema, no existe sistema, 1005 seguro, siempre hay u riesgo que por mucho que lo securices, hay una vulnerabilidad 0 day o cualquier otro riesgo que no puedes mitigarlo 100%. Y aceptas esos riesgos.

BE: Creo que más o menos ya habéis respondido, pero lanzo la pregunta de Nacho: relacionado con la pregunta de Alfonso, al igual que en la vida real hay seguros que cubren los daños que podamos provocar o sufrir, en la industria cibernética, ¿hay alguien que se haga responsable económicamente de un ataque con éxito o que provoque daños graves en una infraestructura digital?

AG: Sí, al final depende de lo aceptado. Depende, por ejemplo, si un caso muy claro, si un atacante se hace con copias de tarjetas de crédito de una entidad bancaria, al final la entidad bancaria tiene potestad para bloquear las tarjetas o no, pero la provee Visa o MasterCard que tienen sus identidades y tienen sus seguros. Los seguros de la vida real aplican aquí, porque hay seguros de tarjetas y si a mi como usuario final, me han robado de mi cuenta porque me han hecho una copia de la tarjeta, al final el seguro de la entidad que me provee de la tarjeta se hace responsable de cubrir los gastos de ese ataque si se demuestra que no he sido yo quien ha hecho esos gastos, esas compras. Al final todo funciona igual.

BE: Iván pregunta: ¿por qué formación tendríamos que comenzar si queremos comenzar nuestra carrera en el mundo de la seguridad digital?

AG: es interesante porque está relacionado con lo que nos hemos dejado por contar, que es nuestra experiencia personal en Accenture. Si sirve de ayuda, que yo creo que sí, yo empecé mi carrera en Accenture y en seguridad el mismo día y fue cuando recibí una llamada estando en pijama en Murcia. No tenía ni idea de todo esto, solo sabía lo que veía en la tele. Esto no va de hackers que saben de todo y aparecen en las noticias que vemos en Internet todos los días. Esto va, como todo en la vida, de mostrar interés por algo y te interese de verdad y que te guste lo que vas haciendo y lo que vas aprendiendo. Pero siempre se parte de la base de que quien empieza no tiene que saber. Además, la ciberseguridad es algo que en ingenierías o formaciones profesionales, no has visto nada de esto en la vida, nunca.

Entonces, no hace falta una formación específica, más allá que las propias ganas que tengas y que te guste a ti aspectos técnicos relacionados. Para empezar. Luego ya, si hay alguien que pueda hacer un curso específico de ciberseguridad, es bienvenido, pero no es algo que… Muchas veces se comete ese error, pensar que sin formación no sirve, y no tiene nada que ver.

AC: relacionado con formaciones sí que hay ciertas formaciones que puedan ayudar. Toda carrera técnica de ingeniería, programación etc. Nos sirven, o son perfiles que van buscados, y tema de masters de cyber, hay unos cuantos. En formato online y en formatos presenciales, tanto en Barcelona como en Madrid y creo que en otros sitios también.

BE: Bueno, Noles pregunta: ¿puede suceder que utilizando un servicio de VPN privado desde un país de leyes más restrictivas se evadan estas a la hora de almacenar la identidad al pensar que viene de un país distinto?

AG: Serían dos cosas distintas porque cuando una identidad se almacena, se almacena en un

sitio físico en concreto, independientemente del modo en el que tú estés accediendo. Si accedes desde una VPN y accedes desde España, pero te mueves a China, será porque probablemente tu identidad esté en China, entonces entrarán en juego dos tipos de legislaciones, aquí en España, qué estés haciendo tú desde donde estás, accediendo a esa VPN, pero una vez que estás dentro de la VPN es probable que apliquen las leyes de lo que estás haciendo en China. Está relacionado, pero no tiene que ver con tu identidad, sino que con la VPN es que accedes desde un sitio.
Por eso es muy importante diferenciar entre gestión de identidades y de accesos. El acceso es a través de la VPN, pero la identidad siempre va a estar en un mismo sitio. Puede ser, pero en este caso no.

BE: relacionado con la pregunta de antes, Jessica pregunta: ¿qué tipo de demanda hay en el sector de la ciberseguridad actualmente?

AC: Eso casi lo puedes responder tú Bea.

BE: bueno, es que va muy en línea con lo que ya habéis respondido. Nosotros como compañía, tenemos dos vías de entrada, lo que ya comentaba Andrés, tenemos contrataciones de gente de talento joven que no tiene experiencia que lo único que necesitamos es ganas de aprender y que se va a formar con nosotros en todo el tema de ciberseguridad, y luego tenemos otros procesos que van más orientados que buscan profesionales con una experiencia más concreta, específica. En estos casos, lo que buscamos es gente que ya aporte conocimientos, no tanto a lo mejor de estudios, titulaciones o certificaciones, sino más experiencia en empresas como la nuestra o en el propio cliente, en áreas específicas de ciberseguridad.

AC: pensad que hay mucha demanda, no sé si es de las que más demanda hay. A nosotros nos llegan ofertas prácticamente a diario

BE: Es cierto, sí.

AG: Y al final es lo que comenta Bea, muy importante que tengáis en cuenta que, por un lado, está la búsqueda de experiencia, esto que todo el mundo sabe, que buscan experiencia, pero si no me dan la oportunidad no puedo ganar experiencia. Esto aquí no existe, si hay gente con experiencia que lleva 5 años, 2 años, 1 año, trabajando en el mundo de la ciberseguridad porque toda experiencia por poco que sea es relevante, pues podrá ser un perfil adecuado para un cargo u otro, pero aquí siempre hay sitio para la gente que quiere aprender y no tiene experiencia, por eso buscan perfiles sin experiencia, como por ejemplo el mío en su momento. Aquí no aplica esto de vale, tengo que hacer esto y esto para que a Accenture le interese mi perfil y entrar a dedicarme a ciberseguridad. Si te interesa hay una opción, si tienes experiencia, según la que tengas, entrarás en un cargo determinado, pero van ligadas, pero no es necesario tener experiencia.

BE: Aunque no lo hemos comentado, abrimos micros para todos aquellos que queráis participar y preguntar directamente. Animaos. Aquellos que habéis lanzado preguntas, si os ha quedado alguna duda o no ha quedado suficientemente aclarado el tema, abrid micro y podemos avanzar o profundizar. ¿Alguien que quiera comentar algo?

Jessica: sí, yo soy Jessica, la que ha hecho la última pregunta. Soy de Bilbao y sé que la sede de Accenture de aquí lleva dos años realizando una formación en ciberseguridad con centros de FP. Yo estoy finalizando mis estudios en DAM, pero visto la situación actual, me estaba planteando la posibilidad de hacer DAW también, aunque son muy parecidas. Y en nuestro centro, hemos estado trabajando con vosotros y quería saber si sabéis si esa formación se va a dar este año y qué opciones hay.

BE: sí, por lo que preguntas es un proyecto que se hizo en conjunto con el gobierno del País Vasco, son acuerdos institucionales que tienen como objetivo eliminar el gap que hemos visto claramente en centros de estudios, tanto universidades como centros de formación profesional, donde se requiere una actualización

de contenidos, para que los titulados nos vengan con conocimientos más acordes a lo que las empresas estamos demandando. Es un proyecto que se lanzó hace dos años, que se va a prorrogar, que nuestro objetivo es mantenerlo, porque nos ha dado muy buenos resultados y Jessica, si todo va bien, pues podremos, como te digo, prorrogarlo al año que viene. En este caso, si te parece, mándame directamente tu currículum, lo movemos y lo coordinamos con la persona que hay en Bilbao en este tema y vamos viendo siguientes pasos perfectamente.

Jessica: vale, muchísimas gracias.

BE: a ti.

AG: Muchas gracias a todos los que ponéis comentarios en el chat. Javier pregunta si la escala es proporcional al riesgo y qué pasa con la centralización y descentralización.
Por un lado, entiendo que lo que preguntas es que si la escala de la arquitectura, si el despliegue de la empresa en sí es más grande, si el riesgo es mayo. Suele ser así, porque no es lo mismo, como comentábamos antes, una tienda que vende libros que Amazon, al final todo depende de la volumetría de usuarios y del público al que esté orientado. No es lo mismo una tienda que vende objetos de un solo tipo, que una tienda que usa todo el mundo para cualquier cosa. Al final todo depende del volumen, con lo cual sí, cuanto más grande sea, mayor riesgo tendrá porque al final será un objetivo más interesante para los atacantes como comentaba Adri, no es lo mismo la gente que vaya a una ferretería online o que compre en una tienda de libros online, que compre en una tienda como Amazon que tienen millones de clientes a lo largo de todo el mundo.
Y el tema de la centralización, pónmelo en el chat si puedes para entender a qué va orientado.

AC: Supongo que al final se refiere a que como estás descentralizando las empresas o las sedes y todo, cómo se interconectan o cómo al final aplicas la seguridad en todos.
Aquí entra mucho el tema de migrar a Cloud, que al final cuando migras a Cloud, tienes tus entornos en un Cloud público o privado y puedes acceder desde cualquier sitio. Y ya estemos nosotros en Barcelona, Andrés y yo, o Bea que está en Madrid, podemos acceder a los mismos recursos porque están públicos desde cualquier sitio.
Y los riesgos son los mismos. Entonces sí que puedes limitar por países, si Accenture no tuviera oficinas en China, pues no hace falta que a sus redes se pueda acceder desde China.

BE: Javier aclaraba en el chat que sí, un blockchain vs. Un servidor central, por ejemplo.

AC: es parecido al final, sí. Puedes… el blockchain en seguridad no se usa mucho, es más pensado en temas de Big Data. ¿Qué te aportaría? Pues más seguridad y que la puedas tener fragmentada, lo único que podrías perder es la… que esté todo fragmentado, todo junto… no me sale la palabra. Sí, que al final perderás, que igual sí que necesitas en algún punto centralizado, el tema muy claro es el de digital Identity, necesitas un directorio y un repositorio de direcciones que esté centralizado, porque si tienes separado por países, por ejemplo, con un blockchain en cada sitio, igual tú te vas y tienes un directorio en España, y cuando te mueves a Francia es otro, con lo que tu usuario ya no está y pierdes esa facilidad de entrar en Amazon Francia porque tu ID está en España.

AG: Además, uno de los ejemplos es justamente Amazon. En FNAC cuando uno de nosotros quiere comprar, la cuenta que tienes en España no es la misma que la de Francia, pero sin embargo la cuenta de Amazon de España, tu cuenta está ahí. Entonces te das cuenta de qué empresas tienen realmente eso pensado para aglutinar las identidades en el mismo repositorio y cuáles no. No se suele pensar en ello, pero se ve claramente cuando te hacen crear una cuenta, porque el repositorio y los sistemas no son los mismos. Amazon claro, son demasiado grandes y están preparados para esto.

BE: Bueno, hay otra pregunta de Nacho, que dice: ¿la seguridad es un trabajo que se puede llevar desde casa para momentos como el que estamos atravesando?

AG: Pues mira, ahí está la cocina. No solo en momentos como este, sino también antes, porque ahora es verdad que la etapa que estamos pasando es complicada para todos,

sea el trabajo que sea. Es verdad que nosotros no solo… puede ser que incluso tengamos más trabajo, sino que podemos llevarlo a cabo desde casa. Pero todos veis en las noticias que

muchas empresas se están dando cuenta de que el teletrabajo existe y funciona. Nosotros ya lo sabíamos antes, ya habíamos trabajado mucho desde casa, sin ningún tipo de problema. Hablando con Adri, nos daba palo, como consultoría de ciberseguridad, que si tenemos que estar todo el día en traje. Me parece que tengo el traje en el armario y lo he puesto tres veces.
Entonces, son cosas que nos gustan mucho porque da sensación de cercanía y donde la quieres ver es en momentos como este. Tienes que trabajar desde casa, y tienes notificaciones y control. Ningún problema, es lo más importante.

AC: Yo llevo de los 4 años en Accenture, los 4 teletrabajando. Lo único que te mueves cuando tienes reuniones con cliente o te toca viajar, o vas a la oficina para quedar con los compañeros.

AG: Al final, lo que te aporta es por lo menos ver a gente. Pero si hay algún tipo de trabajo que se pueda hacer desde casa, es este. Habrá muchos, pero en este no he visto ningún problema.

BE: Hay una pregunta de last minute por aquí. Iván dice: en mi caso personal iba a realizar las prácticas en Accenture Alicante y quería preguntar: ¿cuándo comienzan los periodos de prácticas? ¿Accenture elige unos centros concretos? ¿Hay alguna forma de empezar, nos posicionáis en un puesto según lo académico? Esta pregunta es para mí, te cuento. Cuando hacemos el proceso de selección en la entrevista, recogemos las preferencias, en cuanto a las tecnologías que os gustan, dónde os sentís más cómodos… Y en la medida de lo posible intentamos asignaros a proyectos relacionados. También te digo, en el mundo en el que os ha tocado vivir, sois afortunados, estamos viviendo una revolución tecnológica y hoy en día te va a dar un poco igual. Tu preferencia puede ser estar programando en front con JAVA, cuando en realidad vemos que evoluciona todo tan rápido que vas a necesitar formarte y evolucionar hacia otra tecnología. Nosotros no buscamos gente con conocimientos específicos, buscamos gente con ganas, actitud y capacidad de aprender.
No os preocupéis por eso. Lo que os vamos a ofrecer es una carrera dentro de la compañía, para que podáis encontrar vuestro sitio, teniendo en cuenta lo que os comentaba, que estamos en una revolución y necesitamos gente que siga la velocidad y que vaya evolucionando y aprendiendo distintas tecnologías.

AG: Aquí también Bea, será interesante cuando la gente vaya a aplicar, no solo aquí sino en todos los sitios, dejar constancia de cuáles son tus intereses personales a pesar de que tengas o no experiencia. No es lo mismo alguien que manda el CV a Accenture porque le gusta y quiere dedicarse a un tema que abarca Accenture, que alguien que quiere entrar en Accenture porque sabe que Accenture trabaja la ciberseguridad y le interesa el mundillo. Y no es tanta la gente que hace esas cosas. Entra mucha gente en ciberseguridad que a priori no sabían ni qué le podían gustar.
Mirad la diferencia de alguien que entre sin tener idea en ciberseguridad, si dejas claro que tienes interés y te gusta es diferencial.

BE: Exacto, se recoge en la entrevista y es interesante que nos digáis vuestros intereses. Iván dice: es que en mi caso me encuentro un poco perdido sobre qué estudiar más a fondo, porque me gusta casi todo lo relacionado con el sector. Por eso quería saber si nos asesoráis para iniciarnos en algo concreto.
Yo creo que merece la pena que hagas un ejercicio de lo que comentaba Andrés, qué es lo que te gusta y habrá algo que a lo mejor te motiva más que otro sector o tecnología y sea lo que nos propongas, entonces daremos respuesta y cumpliremos con esas expectativas, y sino Accenture es muy grande, hay muchas áreas y departamentos, y podrás descubrir otras cosas que no tenías en mente y que te pueden resultar interesantes.

AG: de hecho… sí Adri.

AC: Digo que no tengas miedo de equivocarte. Conocemos gente que entró en un sector y se ha cambiado, o haciendo prácticas en un departamento y ha entrado como trabajador en

otro departamento. Al final, hay muchas vertientes y puede ir cambiando de un departamento a otro.

AG: es lo que iba a comentar. Conocemos gente que ahora son compañeros nuestros y llevan mucho tiempo y llevan más que nosotros en Accenture, pero menos que nosotros en Security, que igual estaba en Technology, que por la reestructuración hay más conexión que antes, que se dedicaban a aplicaciones, pero siempre la había gustado la seguridad y ven que tienen una oportunidad dentro de la empresa para meterse en seguridad y acaban entrando en Accenture Security, pese a haber trabajado en Technology haciendo otra cosa.
Todo ligado con tu interés y experiencia, y lo bueno de ser tan grande Accenture es que abarca muchísimos palos distintos. Algunos te pueden interesar y otros menos. No hay problema en probarse y si resulta que, si hay uno que te interesa más que otro, pues intentar moverte.

BE: Había una pregunta de Marta: ¿cómo se encuentran los procesos de selección actualmente? Me encontraba buscando prácticas y se bloqueó todo. No sé cuándo es buen momento para empezar.
Efectivamente, debido a la alerta sanitaria, tuvimos que parar los procesos de estudiantes en prácticas, tanto universidades como FP. Y ahora lo que estamos haciendo es tener una comunicación constante con vuestros propios centros, que son los que nos van dando instrucciones y siguientes pasos, dependiendo de las directrices que a nivel gubernamental y local, se están aplicando en relación a la pandemia. Y en el estado de alerta y cómo va a ser la desescalada.
Estad atentos, preguntad a vuestra persona de referencia y os iremos dando respuesta a medida que nosotros tengamos también la respuesta en este mundo de incertidumbre que estamos viviendo.

Alguien: Hola, ¿se me escucha?

BE: Sí, te escuchamos.

Alguien: en primer lugar, gracias por la charla, me ha parecido bastante interesante y se entendía todo bastante bien. Lo que yo quería comentar es que en mi caso, yo por estas circunstancias, iba a firmar, tenía un contrato con Accenture, contrato laboral, iba a entrar el día 16 y el estado de alarma se puso el 14. Entonces, me pausaron todo, me dijeron que obviamente no podía ir a firmar, y quería más o menos saber cómo va ese proceso, si tengo que esperar, si tengo que ponerme en contacto con alguien…

BE: sí, ponte en contacto con el recruiter que ha estado llevando tu proceso de selección, que es la persona que te irá dando instrucciones de cómo vamos a avanzar con tu proceso. ¿Vale?

Alguien: Ok, muchas gracias.

BE: a vosotros. Ya estamos fuera de tiempo, simplemente, queríamos presentaros las credenciales de la compañía, pero con lo que han contado, mejor nos quedamos aquí. Adri y Andrés lo han cubierto.
Lo que sí que me parecía relevante comentaros es que seguimos haciendo procesos de selección adaptados a las circunstancias. Ahora hacemos todo el proceso online, con lo que hay una fase de nuestro proceso, la dinámica de grupo que hacíamos en la oficina, basada en Lego Serious Play, que no la estamos haciendo, pero que en alguna circunstancia, la hacemos incluso online, con grupos de personas, no es una dinámica de construcción, pero es otro tipo de dinámicas online.
Entonces, para aquellos que todavía no tengamos vuestro CV y queréis participar en los procesos de selección… si pasáis a la última slide… mandadnos por favor un email a eventos-recruiting@accenture.com indicando en el asunto SE-ONLINESEC20, no os preocupéis que cuando os mandemos la… sesión grabada, lo podéis recuperar, indicando que habéis llegado a través de esta sesión, e iniciaremos el proceso. ¿Vale?

Y, por último, habíamos puesto alguna slide relacionada con que os mantengáis en contacto con nosotros, hay multitud de canales que publicamos, pappers, cosas muy interesantes, a la vanguardia de la tecnología y lo que estamos haciendo. Canales donde podéis seguir la actualidad, lo que hacemos y cómo trabajamos en Accenture, que os van a permitir conocernos un poco más.

Bueno, compañeros, yo creo que damos por finalizada la sesión. Todos aquellos que tengáis alguna pregunta, podéis dirigiros a mi correo electrónico. Agradecer la participación de Andrés y Adrián. Muchísimas gracias por vuestro conocimiento, por compartir este ratito con nosotros. Y nada más, muchísimas gracias a todos.

AG: Muy bien, muchísimas gracias.

AC: Muchas gracias, hasta luego.