Observatorio

IDENTIDADES DIGITALES,
EN EL CENTRO DE LA ESTRATEGIA DE SEGURIDAD

La identidad digital se ha convertido en el nuevo perímetro de la ciberseguridad. Los ciberataques dirigidos al robo de las credenciales de los empleados no dejan de crecer, no solo por la relativa facilidad de conseguirlas con técnicas de ingeniería social, sino porque son la puerta de entrada a los sistemas corporativos. Los líderes de ciberseguridad de **Plenitude España, ITP Aero, Donte Group, Sofinco España, Nationale-Nederlanden España, Holcim y Burger King Iberia**, en colaboración con **B-FY**, nos cuentan cómo encaran los nuevos retos para la seguridad de las identidades digitales.

CON EL APOYO DE

B-FY TU BIOMETRÍA SOLO CONTIGO

b-fy.com

TU BIOMETRÍA
SOLO CONTIGO

Cuando no hay datos que robar, deja de ser rentable un ciberataque. Utiliza B-FY.

#FOROITDS

IDENTIDADES DIGITALES, EN EL CENTRO DE LA ESTRATEGIA DE SEGURIDAD

El paso a la nube que ha supuesto la digitalización acelerada de numerosos sectores en los últimos años y la ampliación de la superficie de exposición de las empresas ha llevado a virar las estrategias de ciberseguridad corporativas. La protección y la gestión de las identidades digitales se ha convertido en un elemento básico sobre el que giran las nuevas políticas de seguridad.

A medida que se van haciendo más robustas las soluciones de ciberseguridad de las empresas, crecen los ataques dirigidos al robo de las credenciales de los empleados. Infiltrarse en un sistema bien protegido, con detección temprana de amenazas, análisis de los patrones de comportamiento, autenticación multifactor y políticas de Zero Trust, entre otros elementos, puede ser arduo y costoso. Sin embargo, una campaña de phishing es relativamente sencilla y con ella es posible hacerse con credenciales que den acceso “legítimo” a los sistemas corporativos.

Por ello, los ciberataques dirigidos a identidades en 2023, con intentos basados en contraseñas, se multiplicaron por más de

diez en comparación con el año 2022. Son múltiples los ataques cuyo objetivo es hacerse con los datos de empresas y usuarios para acceder a los recursos corporativos. El robo de credenciales sigue siendo una de las principales vías de entrada de los atacantes, por lo que la identidad se ha convertido en objetivo prioritario y las empresas deben prestar especial atención a su protección.

Para debatir sobre el reto de la gestión de las identidades digitales en el entorno corporativo, en el marco del VI Foro IT Digital Security: Abordando las nuevas fronteras de la ciberseguridad, hemos organizado una mesa redonda con responsables de ciberseguridad de **Plenitude España, ITP Aero, Donte Group, Sofinco España, Nationale-Nederlanden España, Holcim, Burger King Iberia**, con el apoyo de **B-FY**.

LOS NUEVOS DESAFÍOS EN LA PROTECCIÓN DE LA IDENTIDAD

Pese a que se trata de empresas de sectores muy diferentes y tienen casuísticas muy diferenciadas, los desafíos de partida son similares. Por un lado, se ha dejado sentir una mayor sofisticación en los ataques de phishing. Si antes la mayor parte se podían detectar fácilmente por errores burdos en su elaboración, cada vez es más fácil que se tomen como mensajes legítimos.

“Falta concienciación para ceder de por vida un dato biométrico como el iris, teniendo en cuenta que la biometría va a ser el futuro”
Francisco Javier Farfán,
CISO, **Burger King Iberia**

Por otro lado, la digitalización ha llegado a todos los sectores, lo que ha supuesto enormes cambios para la gestión de la ciberseguridad. Si antes muchas compañías mantenían sus sistemas on-prem, en la actualidad la mayor parte ha dado el salto a la nube. A lo que se suman los accesos en remoto en los casos en los que se mantiene alguna modalidad de teletrabajo.

Además, la presencia de los empleados en redes sociales añade un elemento de complejidad. Como señala Cristina Domingo, CISO de Donte Group, “muchas veces queremos compartir mucho relacionado con nuestro día a día. Somos un mundo, ahora mismo, prácticamente digital. Y la gente no es consciente de lo que significa la huella digital: el uso de redes sociales, dónde te estás logando, qué cuentas has creado y qué datos has dado... Te pueden tener totalmente monitorizado, saben dónde estás y lo que haces. Y, también, si has puesto tu cargo y tu empresa”.

LA CONCIENCIACIÓN, LA PRIMERA PIEDRA DE TOQUE DE LA CIBERSEGURIDAD

La capacidad de los empleados para detectar los intentos de phishing y robo de identidad, así como su comprensión más amplia de la seguridad en toda su vida digital, es un elemento fundamental de las estrategias de ciberseguridad. Por ello, la concienciación de los empleados es uno de los básicos en los que trabajan todos los equipos de ciberseguridad de las empresas.

Y es un básico que supone sus propios retos, más o menos variables según el tipo de organización. Las empresas con un gran volumen de empleados tienen que afrontar la

“El arte de la ciberseguridad es muy interesante: tienes que buscar el equilibrio entre dejar al personal trabajar y mantener la seguridad”
Cristina Domingo, CISO, **Donte Group**

complejidad inherente a la cantidad de personas que tienen formar. Teniendo en cuenta además que la orientación que se debe dar según el departamento es diferente, o factores como la alta rotación laboral de algunos sectores o los diferentes niveles de capacitación con los que cuentan los empleados.

Las estrategias para lograr que las tareas de awareness sean efectivas son diferentes. Desde la búsqueda de apoyos imprescindibles en equipos como los de recursos humanos o los de representantes en los distintos equipos que estén pendientes del cumplimiento de las normas básicas hasta campañas de pentesting y hacking ético e incluso la toma de medidas disciplinarias en casos graves.

Un buen ejemplo de esta complejidad lo indica Francisco Javier Farfán, CISO de Burger King Iberia. “Entre los empleados tenemos todo tipo de perfiles, por lo que la concienciación ya no la podemos hacer a nivel corporativo. Por ejemplo, hacemos una concienciación para restaurantes, con un tipo de campañas de phishing, otra para dirección, a su vez dividida por departamentos. Tenemos equipos que nos llevan la parte de concienciación por la cantidad de estatificación que tenemos que ir haciendo”.

LA IDENTIDAD DIGITAL, EL PRINCIPAL ACTIVO QUE PROTEGER

Más allá de la concienciación, el actual escenario digitalizado ha puesto la identidad digital tanto en el foco de los atacantes como en el de las empresas, para las que puede suponer un eslabón débil que acabe provocando infiltraciones y todo lo que puede conllevar: fraudes y secuestro de datos, pérdidas económicas o problemas de imagen, entre otros.

Daniel Damas, head of IT Security de Nationale-Nederlanden España, señala que, si bien “la dinámica de las identidades tiene una carga operativa muy compleja, tienes que poner la identidad digital en el centro para poder controlar los datos, que es por donde hay riesgo. Aparte de las

“La ciberseguridad es un problema de ciudadanía y conciencia social, debería enseñarse concienciación digital con temas básicos”
Daniel Fernández,
Global IT Security officer, **Holcim**

políticas de awareness, nosotros tenemos numerosas capas de seguridad adicionales porque si se logra robar una identidad, los hackers tendrían un acceso legítimo a través de ella".

El cambio de un entorno local cerrado al mundo de la nube ha cambiado la perspectiva de la identidad. Izaskun Onandia, head of Security & Information Compliance de ITP Aero, recuerda que "cuando estábamos on-prem, estábamos como en una burbujita: ponías tu perímetro y no dejabas que se entrase. Pero ahora ya estamos en el cloud, estamos en casa, estamos en todos lados, con lo cual incluso la seguridad ha cambiado. Si antes los controles que eran estáticos, ahora tenemos que poner controles dinámicos y el principal control que tenemos que poner es sobre la identidad".

"La ciberseguridad tiene que ser un acompañador del negocio, es la novia del negocio: sin seguridad, no hay negocio"

Izaskun Onandia, Head of Security & Information Compliance, **ITP Aero**

UN ESCENARIO DE COMPLEJIDAD CRECIENTE

Así, la gestión de las identidades se ha convertido en un elemento clave de las estrategias de ciberseguridad. La complejidad de diseñar, implementar y mantener un sistema de gestión de identidades, basado en políticas de acceso Zero Trust, supone un gran reto. Mayor cuanto mayor sea el volumen de empleados, pero también se ve impactado por los cambios organizacionales, desde las altas y bajas hasta el personal que cambia de equipo, y por la experiencia de usuario que tienen los propios empleados.

Flavio Carvalho, CISO de Sofinco España, considera que "toda la cuestión de las identidades está dentro del tema más amplio de la gestión de riesgos. Uno tiene que chequear en qué nivel está y cómo puede evolucionar. Si en una campaña de fake phishing hay un clic rate muy elevado, identificas los puntos específicos en los que tienes que trabajar".

"Tienes que ir ajustando el sistema de ciberseguridad para que la experiencia del usuario sea grata y no genere rechazo"

Daniel Damas, Head of IT Security, **Nationale-Nederlanden** España

Jesús Abascal, CISO de Plenitude España, señala que siguen una estrategia de

“Algunos elementos clave de la protección de la identidad con las políticas de Zero Trust, la estrategia de mínimo privilegio y la monitorización”
Jesús Abascal, CISO, **Plenitude** España

centralización mediante single sign-on. “Monitorizamos todos los accesos. Incluso hemos activado certificados digitales para las aplicaciones más críticas con el fin de tener un doble factor adicional, no solamente validamos al usuario con su login y su MFA, sino también el equipo corporativo con el que se conecta. Así enriquecemos el contexto y garantizamos la identidad del usuario”.

DE LA EXPERIENCIA DE USUARIO A LA IA GENERATIVA

No hay que olvidar que todos estos planteamientos tienen un efecto directo sobre los usuarios, en cuanto a que se perciben como un elemento disruptor en su día a día. Se debe tener en cuenta la experiencia de usuario, aunque primando siempre la ciberseguridad. Daniel Fernández, global IT Security officer de Holcim, pone como ejemplo el bloque del monitor después de un periodo de inactividad. “Es cierto que, a veces, como usuario es un poco frustrante que se te bloquee la pantalla demasiado a menudo. Pero si se deja un equipo desbloqueado, se tiene acceso a todo con un solo clic con los sistemas de single sign-on, por lo que es un riesgo que no se puede correr. No bloquear el equipo es un problema gravísimo”.

Rodrigo Jiménez, managing director de B-FY, destacó precisamente el carácter amigable de su solución: “En el sistema de protección de la identidad que planteamos, el usuario tiene que leer un QR en el punto de acceso. Estamos demostrando en ese momento exacto del tiempo que con su móvil está justo en un lugar preciso. El primer punto es un QR y el segunda es pedir la biometría desde su propio dispositivo móvil. Con esto lo que hacemos es evitar que los hackers vayan contra una base de datos centralizada”.

Otro elemento que se tuvo en cuenta en el desarrollo de la mesa fue la inteligencia artificial. Si bien hubo consenso en cuanto a su enorme capacidad para ayudar en la detección de amenazas y la identificación

“Hemos protegido bastante más el entorno de monitoreo interno de la red e intentamos llevar la inversión en seguridad frente al riesgo”
Flavio Carvalho, CISO, **Sofinco** España

“Al usuario le puedes dar formación, pero siempre busca la forma de facilitar la experiencia: toma en cuenta al usuario”
Rodrigo Jiménez, Managing director, **B-FY**

de comportamientos anómalos, el consejo general es tener mucha precaución con el uso de la IA generativa. Atendiendo, sobre todo, a cuestiones de privacidad y ubicación de los datos, normativa y cumplimiento.

Las compañías buscan las estrategias que mejor se adaptan a las necesidades concretas de su sector y a las características específicas de su negocio para impulsar y mantener unos

USO ADECUADO DE LA BIOMETRÍA. PARAR EL CIBERCRIMEN Y PROTEGER LA PRIVACIDAD DEL USUARIO

Rodrigo Jiménez, director general de **B-FY**

Rodrigo Jiménez, director general de B-FY, presenta las claves del uso de la biometría en los sistemas de identificación para la identidad digital. El experto explica la evolución del cibercrimen en los últimos años, con organizaciones con auténticas estructuras corporativas que ofrecen plataformas de crimen como servicio. La llegada de tecnologías como la inteligencia artificial generativa les ha permitido además ampliar su capacidad de ataque. Y las identidades digitales son uno de los principales objetivos de los ataques.

En este contexto, cada vez se hace más importante para las empresas incorporar capas de seguridad que aseguren la

identidad de las personas que acceden a sus sistemas, como los sistemas biométricos. Rodrigo Jiménez avisa de los riesgos asociados al robo, precisamente, de los parámetros biométricos: “La biometría es lo más preciso que hay, pero si no la uso de una forma adecuada o no tengo un sistema que me proteja ese dato, si al final es robada, el daño es por partida doble”.

Además, es un elemento especialmente delicado desde el punto de vista normativo y si no se maneja bien se arriesgan multas cuantiosas. “La Agencia Española de Protección de Datos recomienda que todo este tipo de tecnologías siempre están bajo el gobierno y el control exclusivo de los usuarios”. A estos elementos se suma el riesgo de tener centralizados los riesgos biométricos.

altos niveles de ciberseguridad. Pero hay factores comunes como la necesidad de buscar de forma constante la concienciación de los empleados y también de hacer que la ciberseguridad y el negocio vayan de la mano.

Y todas ellas coinciden, además, en que la protección de la identidad digital se ha convertido en uno de los elementos fundamentales de sus políticas de seguridad. Incluso más allá del entorno de la ciberseguridad corporativa, la identidad digital es ya parte de nuestra vida cotidiana y requiere una toma de conciencia de cómo la manejamos. ■

CONTENIDO RELACIONADO

VI Foro IT Digital Security

Identificar personas, eliminar el fraude y proteger la privacidad mediante la identificación como servicio

SI TE HA GUSTADO ESTA REVISTA, COMPÁRTELA

MÁS CONTENIDO

FORO it Digital Security

“La Agencia siempre ha tenido vocación pedagógica para fomentar el complimiento de la protección de datos”

Daniel Mercader, Jefe de la División de Innovación Tecnológica de la Agencia Española de Protección de Datos, nos explica en esta entrevista los trabajos de la Agencia en el ámbito de la innovación y sus esfuerzos en la implantación de la cultura de la privacidad.

“La IA se puede utilizar, pero asegurando que los datos no salgan de nuestras propias barreras”

Izaskun Onandia, head of Security & Information Compliance de ITP Aero, nos cuenta en esta entrevista el reto de la ciberseguridad en una empresa de alta complejidad.

“El riesgo de interrupción del negocio apoya la dotación presupuestaria a la ciberseguridad”

Jesús Valverde, IT Manager & CISO de Isemaren, repasa en este entrevista el escenario actual de ciberseguridad, desde el punto de vista de la normativa, la tecnología y el negocio.

“Los grupos de cibercriminales se están profesionalizando cada vez más”

Miguel Tomás Ruiz, subdirector de ciberseguridad de la CNMV, expone en esta entrevista su visión sobre la ciberseguridad y las diferentes normativas que afectan al ámbito financiero y la evolución de las amenazas con tecnologías como GenAI.

ABORDANDO LAS NUEVAS FRONTERAS DE LA CIBERSEGURIDAD

¡Ver todos los contenidos!

PATROCINADORES

COLABORAN