Volumen 1. Numero 1. Serie A

ISBN: 978-99939-0-055-9

CyberSecurity

Información & Privacidad

ISO/IEC 27701

El nuevo estándar global que ayudará a proteger la privacidad

Segmentación basada en la intensión

Solución a un nuevo reto ante la transformación digital

Seguridad de la Información

Un corte transversal a la organización

Https implica seguridad mas no autenticidad

El Certificado en sí, no es el problema

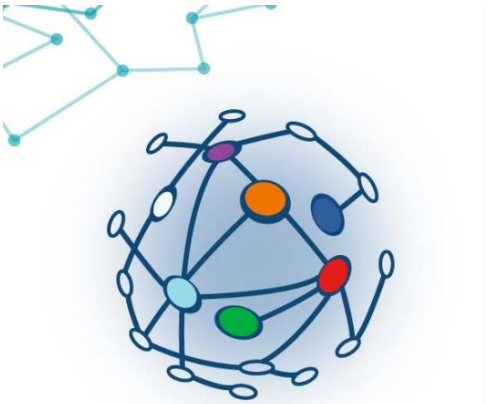
Las lecciones aprendidas de los "Panamá Papers"

Ejemplo de lo que no se debe hacer a nivel organizacional

CyberSecurity

Información & Privacidad

Proyecto de:



ISBN: 978-99939-0-055-9

Publicación de la Asociación Universitaria en Ciencias de la Investigación (AUCI)

Dirección General

AUCI Guatemala

Junta Directiva

2019-2021

Cybersecurity Magazine - Información *y Seguridad*

Universidad Mariano Gálvez de Guatemala
Ing. Daniela de Villatoro
Ing. Criss Velasquez
Ing. Armando Monzón

Diseño:
Ing. Darwin Fuentes

Enero – Abril 2020

Nota del editor

El avance que ofrecen las nuevas tecnologías de la información aportan mejoras y un rápido crecimiento a las pequeñas, medianas y grandes empresas a lo largo del mundo, pero también representa un riesgo para estas en centroamérica y la región, ya que informes demuestran que los ciberataques son algunas de las amenazas de más rápido crecimiento en la actualidad a las que se enfrentan, aspectos como la falta de interés, presupuesto y conocimiento hacen que los ciberdelincuentes se aprovechen de las pocas o nulas defensas de protección y el déficit de profesionales es una preocupación latente para una correcta gestión de riesgos y amenazas internas y externas, por otro lado la utilización de metodologías disponibles para ciber seguridad sigue siendo algo complejo en nuestra región, ya que, se requiere un nivel de madurez real para abordar estos aspectos de mejora dentro de la empresa.

Cybersecurity – "Información y Privacidad" nació de la idea de dar oportunidad a los profesionales para publicar artículos de alto nivel y que sean leídos no solo por los contactos en las redes sociales sino se llegue a más profesionales que buscan contenidos fiables, futuristas y de interés y con esto crear una red profesional exponiendo sus investigaciones y experiencias acerca de ciberseguridad al mundo.

Les invito a leer, compartir y comentar los artículos que en esta revista se exponen, pueda ser que en un futuro cercano también compartas conocimientos y experiencias en Cybersecurity – "Información y Privacidad".

Ing. Cristina de Monzón

CyberSecurity
Información & Privacidad

Artículos

ISO/IEC 27701, el nuevo estándar global que ayudará a proteger la privacidad

ISO / IEC 27701, the new global standard that will help protect privacy

Juan Carlos Morales
email: juancarlos.moralesbathen@yahoo.com
Recibido:15/enero/2020. Revisado: 25/enero/2020. Aprobado: 15/Febrero/2020.
Disponible en internet el 1 de marzo de 2020

Resumen: La ISO 27701 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Información de Privacidad. Esta normativa se basa en los requisitos, controles y objetivos de los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI). Una de las ventajas que ofrece esta nueva certificación radica en que la organización podrá compatibilizar el cumplimiento en materia de seguridad de la información y privacidad, ya que posibilita integrar la normativa en materia de protección de datos del país donde se implemente y reforzar las medidas técnicas y organizativas

Palabras Claves: Privacidad, estándar, normativa, seguridad.

Abstract: ISO 27701 specifies the requirements to establish, implement, maintain and continually improve a Privacy Information Management System. This regulation is based on the requirements, controls and objectives of the requirements of the Information Security Management System (ISMS). One of the advantages offered by this new certification is that the organization will be able to make compliance in the area of information security and privacy compatible, since it makes it possible to integrate the data protection regulations of the country where it is implemented and to reinforce technical measures. and organizational

Desarrollo:

¿Qué sabemos acerca de la privacidad de nuestra información? ya que constantemente se nos pide que ingresemos la dirección de correo electrónico, número telefónico, nombre y apellido en plataformas tecnológicas, además que algunas de estas incluso obtienen acceso a nuestras coordenadas por medio de GPS.

Cuando alguien gana acceso a nuestros datos, puede acumularlos, analizarlos y no sabemos que uso puede darles en un futuro, información compartida sin control podrían ocasionar discriminación por raza, religión o por condición de salud entre otros. Algunos casos pueden ocasionar pérdidas financieras por divulgación de datos y contraseñas relacionadas con tarjetas de crédito, débito o cuentas bancarias y la información puede quedar expuesta a personas que roben la identidad o comprometan la imagen o reputación que podrían utilizarse en extorsiones o en delitos relacionados al robo de información que comprometan la integridad de las personas.

En los Estados Unidos se utiliza el término información personal identificable el cual se abrevia como PII. El Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST: National Institute of Standards and Technology) (Digitalguardian.com, 2018) proporciona la siguiente definición: PII es cualquier información que pueda usarse para distinguir o rastrear la identidad de un individuo, tal como nombre, número de seguridad

social, fecha y lugar de nacimiento, apellido o registros biométricos; y cualquier otra información que pueda vincularse como correo electrónico, información médica, educativa, financiera y de empleo.

Los datos personales se consideran el equivalente europeo a PII, aunque difiere un poco con la definición anterior. El Reglamento general de protección de datos de la Unión Europea (GDPR) (AEC.es, 2018)define los datos personales de la siguiente manera:

Datos personales significa cualquier información relacionada con una persona física identificable por referencia a un identificador, tal como un nombre, un número de identificación, datos de ubicación, un identificador online, o a uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, social o cultural de la persona natural.

Como consecuencia de la acelerada transformación digital y del creciente aumento del uso de la información personal, la protección de esta se ha convertido en una necesidad social, llevando a tener que establecerse regulaciones y leyes al respecto. Por tal motivo las obligaciones legales se han vuelto cada vez más estrictas. La protección de nuestra privacidad digital una preocupación comercial importante y se ha iniciado una nueva era de regulación y cumplimiento de la privacidad en todo el mundo. Muchas organizaciones no están preparadas actualmente, pues carecen de directivas y procedimientos para asegurar el cumplimiento de las recientes normativas de privacidad. Esto ha aumentado las quejas y multas relacionadas con la protección de datos.

Para dar orientación a nivel global, en agosto del 2019 se publicó el estándar sobre protección de la información personal, el cual forma parte de la amplia familia de normativas ISO/IEC 27000 sobre seguridad de la información. ISO/IEC 27701 (ISO.org, 2019)puede considerarse como una extensión de ISO/IEC 27001 (pmg-ssi-com, 2017) e ISO/IEC 27002. Su objetivo es proporcionar orientación sobre la protección de la privacidad, y la forma en que las organizaciones deben gestionar la información personal para aumentar la confianza y transparencia de las partes interesadas.

ISO/IEC 27701 está conformado por 8 cláusulas y 6 anexos, que incluyen controles de información de identificación personal y mapeos a normas relacionadas tales como ISO / IEC 29100:2011 Marco de Referencia para la Privacidad, ISO / IEC 27018:2019 Código de Prácticas para la Protección de la Información de Identificación Personal (PII) (Imperva.com, 2018) en la nube, ISO / IEC 2915:2017 Código de Prácticas para la Protección de la Información de Identificación Personal, y al Reglamento General de Protección de Datos de la Unión Europea.

El estándar tiene validez a nivel internacional, pero debe ser interpretado para tomar en cuenta la legislación y normativa de cada país. Es aplicable a todos los tipos y tamaños de organizaciones, incluidas empresas públicas y privadas, entidades gubernamentales y organizaciones sin fines de lucro.

ISO / IEC 27701 fue desarrollado por el comité técnico ISO / IEC JTC1 / SC 27, Seguridad de la información, ciberseguridad y protección de la privacidad, que está compuesto por expertos de todo el mundo de las autoridades de protección de datos, agencias de seguridad, academia e industria. Especifica los requisitos y proporciona orientación para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de privacidad de la información (PIMS) dentro del contexto de la organización.

Referencias bibliográficas

AEC.es. (2018). Obtenido de https://dpd.aec.es/nueva-iso-iec-277012019-integracion-del-rgpd/

Digitalguardian.com. (2018). Obtenido de https://digitalguardian.com/blog/what-nist-compliance

Imperva.com. (2018). Obtenido de https://www.imperva.com/learn/data-security/personally-identifiable-information-pii/

ISO.org. (2019). Obtenido de https://www.iso.org/standard/71670.html

pmg-ssi-com. (2017). Obtenido de https://www.pmg-ssi.com/2019/09/nueva-iso-iec-277012019/

Sobre el autor:

Más de 30 años de experiencia profesional en Tecnología de la Información colaborando con instituciones bancarias y con multinacionales como Shell Royal Dutch, Bayer y Wal-Mart. Ingeniero en Sistemas y Magister Artium en Administración de Empresas con especialidad en Mercadeo. Ha sido catedrático universitario, escritor, y posee las certificaciones CISA, CISM, CRISC y CGEIT.

Segmentación basada en la intención.

Intention-based targeting

Obdulio Sierra
email: osierra@fortinet.com
Recibido:13/enero/2020. Revisado: 27/enero/2020. Aprobado: 12/Febrero/2020.
Disponible en internet el 1 de marzo de 2020

Resumen: Cada vez más, las arquitecturas tradicionales de las redes de centros de datos y de las empresas están siendo obligadas a adaptarse rápidamente a estos requerimientos dinámicos. Las aplicaciones se están moviendo hacia entornos de nube pública, privada o híbrida, donde ahora son consumidas como servicios; lo que dificulta cada vez más distinguir las barreras entre las redes empresariales y los dominios que no son dignos de confianza. Para mantenerse al nivel de estas tendencias, es necesario que evolucionen las infraestructuras de red de centro de datos y de las empresas, al igual que sus respectivos procedimientos operacionales.

Palabras Claves: Ciberseguridad, transformación digital, infraestructura, amenaza, conectividad.

Abstract: Increasingly, traditional enterprise and data center network architectures are being forced to quickly adapt to these dynamic requirements. Applications are moving to public, private, or hybrid cloud environments, where they are now consumed as services; making it increasingly difficult to distinguish barriers between business networks and unreliable domains. To keep up with these trends, business and data center network infrastructures need to evolve, as do their respective operational procedures.

Desarrollo:

Algunos de los mayores retos que plantea la transformación digital es la seguridad de las redes, el perímetro y una aplicación de la segmentación como segunda línea de defensa para reducir la superficie de ataque y evitar la propagación lateral de las amenazas que se vuelven más complejas, ya que han quedado difusas dentro de las mejoras en las nuevas organizaciones, como por ejemplo la movilidad, el Internet de las cosas, el uso de la nube y el "Shadow IT" (GB-Advisors, 2018), entre otros ya que son el pan de cada día de los administradores de las tecnologías en la actualidad.

Una solución a este reto es la segmentación basada en la intención, que no es más que la capacidad de una red en poder identificar los dispositivos que se conectan a la infraestructura según su naturaleza, y con esto aplicar políticas de seguridad en forma dinámica; sin importar su ubicación en la red. (borde, centro de datos o incluso en la nube).

Las redes de hoy en día deben tener la capacidad de ejecutar en forma automatizada, evaluaciones periódicas de seguridad y el nivel de riesgo para asignar la conectividad adecuada y políticas de seguridad a los activos en la red. Una estrategia (Acis.org.co, 2018) adecuada de integración entre los componentes de red y los sistemas de seguridad a todo nivel facilitara la gestión y configuración.

De esta forma, mediante la segmentación basada en la intención, la estrategia ya no es solo hacer una segmentación "geográfica" según la ubicación de los activos conectados en la red, sino más bien utilizar dispositivos de seguridad de red ubicuos con capacidad de analizar el

tráfico encriptado que ya es mayoría, y aplicar políticas hasta capa 7 (Cloudfare.com, 2017) sin comprometer el rendimiento de la red, esto sin requerir cambios en la arquitectura o cambio de equipos.

Estos dispositivos deberán integrarse con los dispositivos de conectividad de red, las herramientas de analítica y detección de amenazas de la organización. Toda esta integración debe permitir "etiquetar" los activos de la organización de tal forma que sean fácilmente identificables según su naturaleza para el negocio y las políticas viajen con ellos independientemente de su ubicación en la red. Un ejemplo podría ser identificar todos los activos que están relacionados con el cumplimiento de una normativa en particular, o los que son de vital importancia para la operación de determinado sistema o departamento.

Toda la red, deberá tener la capacidad además de poder rápidamente detectar un dispositivo comprometido, ya sea por una amenaza de día cero o una amenaza (Alcaldia Mayor Bogotá, s.f.) conocida y aislarlo en forma automatizada sin la necesidad de intervención humana, evitando de esta forma, la propagación lateral de las amenazas y una afectación en el negocio.

Para implementar la segmentación basada en la intención en la red, deben considerarse entonces los siguientes elementos:

• Visibilidad y auditoria constante. Se deben integrar mecanismos que permitan auditar constantemente el cumplimiento de buenas prácticas de seguridad, así como la salud de los componentes de la red y los dispositivos conectados.

• Mecanismos de etiquetado. La red debe ser capaz de identificar y etiquetar los activos de la red según la lógica del negocio.

• Control granular de acceso. Debe ser capaz de definir por tipo de dispositivos, usuarios o aplicaciones, cuando pueden conectarse y en que parte de la red.

• Respuesta automática a incidentes. Mediante la integración de la infraestructura de seguridad y red con plataformas analíticas que correlacionan los eventos locales y a su vez se conectan con fuentes externas de reputación, la red debe automatizar el proceso de respuesta a incidentes de seguridad.

Referencias bibliográficas

Acis.org.co. (2018). Obtenido de http://acistente.acis.org.co/typo43/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/16-PlaneacionEstrategicaSeguridad.pdf

Alcaldia Mayor Bogotá. (s.f.). Obtenido de http://199.89.55.129/scorecolombia/documents_co/herramientas/M5/Material_tecnico_apoyo/SGSST_2015/3.%20Planificaci%C3%B3n/5.%20Plan%20de%20Emergencias/Cartillas/Cartilla_Amenaza_Tecnologica_DPAE.pdf

Cloudfare.com. (2017). Obtenido de https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

GB-Advisors. (2018). Obtenido de https://www.gb-advisors.com/es/shadow-it/

Imperva.com. (2018). Obtenido de https://www.imperva.com/learn/data-security/personally-identifiable-information-pii/

Sobre el autor:

Asesor en tecnología, con más de 20 años de experiencia, ingeniero en sistemas por Universidad Galileo y MBA con especialización en marketing por la Universidad Francisco de Vitoria. También ha obtenido algunas certificaciones de fabricantes como Cisco CCNA y el Fortinet NSE4. En su carrera profesional ha laborado en diferentes roles de ingeniería y comerciales para empresas multinacionales como Telefónica, McAfee y Microsoft. Actualmente se desempeña como responsable de país para Fortinet en Guatemala.

CyberSecurity
Información & Privacidad

Seguridad de la información: un corte transversal a la organización

Information security: a cross section of the organization

Delorean Randich
email: drandich@columna.com.gt
Recibido:16/enero/2020. Revisado: 26/enero/2020. Aprobado: 15/Febrero/2020.
Disponible en internet el 1 de marzo de 2020

Resumen: Cada vez más, las arquitecturas tradicionales de las redes de centros de datos y de las empresas están siendo obligadas a adaptarse rápidamente a estos requerimientos dinámicos. Las aplicaciones se están moviendo hacia entornos de nube pública, privada o híbrida, donde ahora son consumidas como servicios; lo que dificulta cada vez más distinguir las barreras entre las redes empresariales y los dominios que no son dignos de confianza. Para mantenerse al nivel de estas tendencias, es necesario que evolucionen las infraestructuras de red de centro de datos y de las empresas, al igual que sus respectivos procedimientos operacionales.

Palabras Claves: seguridad de la información, organización, gestión, riesgos, tecnología.

Abstract: Increasingly, traditional enterprise and data center network architectures are being forced to quickly adapt to these dynamic requirements. Applications are moving to public, private, or hybrid cloud environments, where they are now consumed as services; making it increasingly difficult to distinguish barriers between business networks and unreliable domains. To keep up with these trends, business and data center network infrastructures need to evolve, as do their respective operational procedures.

Desarrollo:

Confidencialidad, integridad y disponibilidad, tres términos que son recitados con la técnica y la teoría mediante el estándar internacional ISO 27001, el cual pretende el establecimiento de un sistema de gestión de seguridad de la información; pero, realmente en el contexto corporativo y práctico, ¿cuál es el verdadero significado de este planteamiento? Esto es lo que, desde el punto de vista estratégico y de auditoría interna, se pretende exponer en el presente artículo.

Antes que nada, una certificación internacional o bien, el mismo establecimiento de un sistema de gestión de seguridad de la información, no debería ser otro tema, más que el resultado de la afirmación de un compromiso institucional desde el nivel de toma de decisiones hasta las instancias operativas, y cuyo beneficio constituya un elemento tangible de generación de valor y factor diferenciador de la institución que lo implemente, ante sus pares; ya sea esto en el ámbito privado, estatal, o de cotización bursátil.

El Foro Económico Mundial, a través del Informe Global de Riesgos se ha encargado de expresar anualmente, al menos desde hace ya varios años, la dimensión e importancia que tienen los diferentes ambientes de riesgo ante la sociedad en general, y en auge los últimos años los riesgos de ciberseguridad y fraude en la información; y de manera muy curiosa, una baja significativa en el perfil de estos riesgos en el informe del año 2020, en donde se exponen

como de vital importancia temas de desastres naturales, pérdida de biodiversidad, armas de destrucción masiva, eventos climatológicos extremos, entre otros.

En dicho sentido, la seguridad de la información debe constituir una filosofía de índole estratégico, más que un tema técnico, como muchos opinarían; en virtud de representar el resguardo y la adecuada gestión de la información, y sus diversas manifestaciones de sensibilidad; no sólo de sus clientes, sino del amplio espectro de grupos de interés que girar alrededor de la operación. Más aún, en una actualidad disruptiva en donde la tecnología, la innovación, la estrategia, y la interrelación de estos tres elementos son el presente y el futuro de todas las organizaciones, y en cuanto más responsable sea una institución, no sólo en la aceleración de estas tres fuerzas, sino en la gestión adecuada de los riesgos que esta realidad representa; los réditos serán consecuentes con la alineación y superación de las expectativas de sus stakeholders.

Mucho se narra respecto de las profesiones del futuro o de las actividades obsoletas, en donde se proyecta una inclinación hacia habilidades de innovación tecnológica y de ciertas softskills, sin embargo, el denominador común de un líder en el campo “profesional”, será determinando en el sentido de observar a la institución desde un foco panorámico y con un corte transversal, saliendo del enfoque tradicional, que cita a la cadena de valor como el eslabón más fuerte, por el contrario, implementar no sólo actitudes de promoción en materia de ciberseguridad, sino, el movimiento de un engranaje que compatibilice los procesos de decisión estratégica, el core business, y las actividades de apoyo.

La actividad profesional de auditoría interna, como un aliado estratégico, unido en la misión de agregar valor en todos y cada uno de los procesos de la institución deberá ser un promotor dinámico en la observancia permanente de los riesgos inherentes que trae consigo la realidad presente de innovación tecnológica.

En este contexto, la Fábrica de Pensamiento, el think tank del Instituto de Auditores Internos de España ha abordado en varios documentos las diferentes manifestaciones de los riesgos cibernéticos, tanto por medio de fraude dinerario, robo de información, indisponibilidad de servicios, pérdida de reputación, sabotaje de infraestructuras, entre otros. Lo anterior con un potencial a ser perpetuado por diferentes perfiles de los atacantes (hacking, cibercrimen, hacktivismo, ingeniería social, ciberespionaje, insiders y ciberterrorismo). Elementos con un aumento exponencial, no sólo por los conceptos planteados en el presente artículo (innovación tecnológica y disrupción), sino, expuestos de una forma latente por el auge de tecnologías de índole financiero tales como, las criptomonedas, blockchain y las fintech, nuevas aristas que representarían no sólo riesgos organizacionales, más bien, riesgos sistémicos para economías a nivel internacional

Referencias bibliográficas

"A well-informed sense of assurance that information risks and controls are in balance." (Anderson, J., 2003)

"Information security is the protection of information and minimizes the risk of exposing information to unauthorized parties." (Venter and Eloff, 2003)

The Government of the Hong Kong. An Overview of Information Security Standards. 2008. Hongkong.

Overview on COBIT. http://www.benchmarklearning.com/COMMUNITIES/ITIL/cobit.aspx

Overview on British Standard. http://www.bsigroup.com/en/Standardsand-Publications/About-BSI-British-Standards/

http://www.isaca.org/KnowledgeCenter/COBIT/Pages/Overview.aspx

http://www.iso.org/iso/about/discover-iso_isos-name.htm

Sobre el autor:

Más de 12 años de experiencia en el sector asegurador y auditoría. Es Contador Público y Auditor por la Universidad de San Carlos de Guatemala USAC (actualmente en curso PhD en Derecho), también cuenta con un MBA por Universidad Galileo. Ha sido speaker en conferencias gremiales y participante en eventos en Guatemala, Costa Rica, Panamá y Estados Unidos. Cuenta con más de 900 horas de vuelo en disertaciones en materia de auditoría interna, gestión de riesgos, gobierno corporativo y materias afines. Actualmente se desempeña como Auditor Interno en Seguros Columna, aseguradora del sistema MICOOPE. Es catedrático en la Facultad de Ciencias Económicas USAC, miembro activo del Instituto de Auditores Internos, Instituto Guatemalteco de Contadores Públicos y Auditores y Colegio de Contadores Públicos y Auditores de Guatemala, también es Directivo Nacional de Habitat para la Humanidad Guatemala. Ha sido acreedor al reconocimiento por la mejor tesis del año con el tema “Solvencia II en una compañía de seguros guatemalteca”.

CyberSecurity
Información & Privacidad

HTTPS implica seguridad mas no autenticidad

HTTPS implies security but not authenticity

Rodrigo Calvo
email: rcalvo@infolock.com
Recibido:18/enero/2020. Revisado: 22/enero/2020. Aprobado: 13/Febrero/2020.
Disponible en internet el 1 de marzo de 2020

Resumen: Los ataques tipo “phishing” lejos de disminuir se mantienen en el tiempo y aumentan en complejidad; el factor común entre los incidentes radica en que el cibercriminal usa estrategias para atraer la atención de su público meta en las que pueda minimizarse la percepción de engaño. El problema radica en que, históricamente la aparición de las siglas “https” para los usuarios implica seguridad e indirectamente autenticidad. Los certificados SSL aseguran el transporte de la información de tal manera que se mantenga la privacidad de la transacción entre el navegador de internet y el servidor web destino. La venta de dichos instrumentos de aseguramiento web ofrece alternativas que van desde uso gratuito hasta prueba de evaluación por un número limitado de días, sin embargo, dicho proceso comercial permite un uso malicioso de la tecnología en donde individuos diseñan estrategias de phishing con el objetivo final de obtener credenciales de usuarios bajo engaño. Comprender la dimensión del phishing bajo las ópticas de identificación, remediación y reporte de incidentes será el foco primario del artículo.

Palabras Claves: certificado digital. Seguridad, autenticación, tecnologia, internet.

Abstract: Phishing-type attacks, far from diminishing, are maintained over time and increase in complexity; The common factor among the incidents is that the cybercriminal uses strategies to attract the attention of his target audience in which the perception of deception can be minimized. The problem is that, historically, the appearance of the abbreviations "https" for users implies security and indirectly authenticity. SSL certificates ensure the transport of information in such a way that the privacy of the transaction between the internet browser and the destination web server is maintained. The sale of these web assurance instruments offers alternatives ranging from free use to evaluation tests for a limited number of days, however, this commercial process allows malicious use of technology where individuals design phishing strategies with the ultimate goal. to obtain user credentials under deception.

Desarrollo:

El ataque comienza como un correo electrónico que solicita información del usuario en nombre de un departamento interno para autenticar un nuevo dispositivo o para proporcionar un “documento importante". En otras palabras, el correo electrónico proporciona un requisito falso para tomar ventaja sobre los usuarios. Al usuario promedio se le ha enseñado que identificar "https" junto a la URL de un sitio web significa que el sitio es seguro, especialmente cuando se realizan transacciones en línea. Las recomendaciones generales o mejores prácticas disponibles apuntan al hecho de que, el cifrado de las páginas web sirve como un medio seguro. Muy a menudo se escuchan sugerencias como: "Cuando se le solicite enviar información personal confidencial, una dirección web genuinamente segura debería

comenzar con https://", También hay otras sugerencias similares a "Verificar la dirección del sitio web: la página de inicio de sesión en el sitio web de su banco debe comenzar con https", y entre otras más, "Al iniciar sesión en sitios bancarios, de compras y de correo electrónico, siempre busque https al comienzo de la URL. La ‘S' significa seguro”.

Se ha advertido constantemente a los usuarios, que estén atentos a las estafas de phishing y que examinen de cerca las URL o los dominios que acompañan a los mensajes sospechosos. Un ejemplo muy familiar de un ataque de phishing es un correo electrónico supuestamente del Banco que solicita ingrese a un sitio para actualizar sus datos sin embargo el remitente proviene de Gmail u otra dirección no corporativa.

La siguiente etapa orquestada por los piratas informáticos requiere que el usuario final haga clic en un botón de acción disponible en el correo electrónico. Una nueva sesión del navegador web se abre inmediatamente al solicitar las credenciales del usuario. La sesión parece segura para un usuario normal, ya que incluye “https” y un ícono de candado. El fallo en la estrategia seguida se debe a que el dominio no está relacionado con el sitio oficial, pero, el fondo de la página y el símbolo de candado hacen dudar al usuario lo suficiente como para digitar sus credenciales. En este caso específico, el certificado SSL parece estar validado en el dominio y tiene una característica especial: Un certificado SSL a costo cero durante 90 días. Un certificado regular mostrará que es válido en un rango de no menos de un año.

Se han encontrado otros casos de uso completamente gratuitos, proporcionados por el Grupo de Investigación de Seguridad de Internet (por sus siglas en inglés ISRG) y su iniciativa llamada Let's Encrypt, la cual proporciona certificados digitales de forma gratuita (es uno de sus postulados claves, el libre acceso a los certificados por parte de cualquiera). La información anterior es consistente con un artículo de Robert Duncan, donde menciona: "El uso de TLS por parte de estos sitios de phishing es particularmente peligroso, ya que los sitios web que usan TLS son comercializados como confiables y operados por operaciones legítimas. Los consumidores han sido entrenados para buscar candados, indicadores de seguridad y https:// en la barra de direcciones de su navegador antes de enviar información sensible, como contraseñas y números de tarjetas de crédito a los sitios web ".

Como parte de la investigación realizada por el autor, se contactó al soporte técnico de una conocida Autoridad Certificadora (CA) para conocer la opinión sobre situaciones como esta y la respuesta fue la siguiente: “Un certificado SSL / TLS correctamente instalado y configurado garantiza que las transacciones a través del sitio web de un proveedor sean seguras y estén hechas de tal manera que se está a salvo de la influencia de terceros. Un CA no regula, controla ni supervisa las prácticas comerciales de ningún operador de sitio web, ni nuestros servicios se relacionan de ninguna manera con el contenido de un sitio web en particular. No podemos garantizar que los operadores actuales de los sitios actúen siempre con integridad y honestidad en [sus] negocios con el público. En última instancia, los consumidores aún deben decidir en qué proveedores se debe confiar y tratar en línea antes de realizar cualquier tipo de negocio allí. Las garantías de CA no pueden cubrir transacciones en las que se haya juzgado mal las intenciones del propietario del sitio o donde el propietario del sitio haya actuado mal”

Si la empresa desea habilitar un sitio de comercio electrónico en el cual se solicita información de identificación personal o para recibir la información confidencial, un certificado digital de evaluación o prueba SSL no debería ser una opción porque la validación de la propiedad del sitio es básica y limitada.

Las recomendaciones de expertos indican que para adquirir un Certificado Digital se debe de pensar en Validación Extendida (EV SSL) es la nueva norma; el costo por año es de entre $225 y $ 600 por certificado. De acuerdo con las Autoridades de Certificación / Foro de navegadores (también conocido como CA | B), los beneficios adicionales de EV SSL son:

Hacer que sea más difícil montar phishing y otros ataques de fraude de identidad en línea mediante el uso de certificados.

Asistir a las organizaciones de cumplimiento de la ley en sus investigaciones en temas de fraude electrónico y otros fraudes de identidad en línea, que incluyen (cuando corresponda) el contacto, la investigación o la adopción de medidas legales contra el tema. Reciba una garantía, que ofrecen ciertos certificados pagados.

Utilizar una tecnología basada en el perímetro, como un Proxy seguro o tecnologías basadas en la nube capaces de identificar y prevenir la inserción de URL sospechosas en un correo electrónico. Utilizar la autenticación de dos factores (2FA) integrados para dificultar el acceso a una cuenta simplemente con el uso de una contraseña.

Proporcionar capacitación a los usuarios y, si es posible, hacer pruebas con ataques de phishing simulados. Reportar cualquier correo electrónico sospechoso al departamento de seguridad de TI de su empresa. Seguridad de TI e Informar cualquier certificado que se utilice en un ataque de phishing a la Autoridad de Certificación del remitente y solicite la revocación de su certificado. Los certificados SSL basados en dominio, es decir aquellos que solamente se adquieren sin aportar evidencia de persona física o jurídica, no aportan criterios de autenticidad o propiedad del sitio web, únicamente cifran el canal de comunicación.

Con las versiones de prueba de los certificados, los proveedores buscan fijar la necesidad en sus clientes de adquirir el servicio oficial al finalizar el periodo de noventa días, no obstante, de manera indirecta permiten gratuitamente a cibercriminales implementar ataques de phishing con niveles mayores de engaño.

Las entidades que ofrecen algún tipo de transacción en línea mejorarían su imagen y la protección de la información de sus clientes al hacer uso de certificados de validación extendida y también al informar ampliamente sobre la forma correcta de identificar si se está accediendo al sitio transaccional correcto.

Los usuarios deben dejar de pensar que un candado y https en el navegador ofrecen suficientes pruebas de seguridad para ingresar sus credenciales, pagos o información privada sin investigar más si el propietario es real.

Referencias bibliográficas

Rodrigo Calvo. (2018,3 de Agosto). The True Cost of Certificate Authority Trials: Can You Trust Them?. Disponible en: https://www.isc2.org/News-and-Events/InfoSecurity-Professional-Insights-Archive/2018%20Archived%20Content/August-2018

Robert Duncan. (2017,17 de Abril). Let's Encrypt and Comodo issue thousands of certificates for phishing. Disponible en: https://news.netcraft.com/archives/2017/04/12/lets-encrypt-and-comodo-issue-thousands-of-certificates-for-phishing.html

*CA/Browser Forum. (2013, 4 de Septiembre).*About EV SSL: Objectives of Extended Validation. Disponible en https://cabforum.org/about-ev-ssl/

Sobre el autor:

Consultor Internacional de Ciberseguridad con más de 15 años de experiencia, Certificado e Instructor Autorizado en Information Systems Security Professional (CISSP) así como de Ethical Hacker (CEH) , profesor en la Maestría de Ciberseguridad de la Universidad Cenfotec en Costa Rica, Miembro de la Junta Directiva del Capítulo (ISC)2 Costa Rica, Speaker en Congresos de Protección de Datos y Ciberseguridad, actualmente labora como Arquitecto Senior de Seguridad de la Información en la compañía Infolock, Virginia , Estados Unidos , anteriormente fue Sr. Security Engineer en Symantec Corp Latinoamérica.

CyberSecurity
Información & Privacidad

Las lecciones Aprendidas de los “Panamá Papers”

The Lessons Learned from the “Panama Papers”

Luis Gorgona
email: lgorgona@gmail.com
Recibido:19/enero/2020. Revisado: 24/enero/2020. Aprobado: 10/Febrero/2020.
Disponible en internet el 1 de marzo de 2020

Resumen: El escándalo de "Papeles de Panamá" reveló un problema latente que existe en la mayoría de las empresas hoy en día: el robo de información comercial, vital y la imposibilidad de contenerlo o evitarlo. Esto tiene un efecto adverso en las organizaciones desde el daño financiero hasta el de reputación, las implicaciones, los errores típicos y como evitar que esto suceda en una empresa. Lo que sucedió en la firma legal panameña es un ejemplo de lo que no se debe hacer a nivel organizacional, algo a lo que todos los empresarios, gerentes y miembros de la junta deben prestar atención, los errores cometidos no se limitaron a los sistemas específicos involucrados o los datos confidenciales particulares que se filtraron; más bien, el incidente surgió de errores estratégicos y organizacionales.

Palabras Claves: Confidencialidad, reputación, organización, riesgo, ciberseguridad.

Abstract: The "Panama Papers" scandal revealed a latent problem that exists in most companies today: the theft of commercial, vital information and the impossibility of containing or avoiding it. This has an adverse effect on organizations from financial damage to reputational damage, implications, typical mistakes and how to prevent this from happening in a company. What happened in the Panamanian law firm is an example of what not to do at the organizational level, something to which all businessmen, managers and board members must pay attention, the mistakes made were not limited to specific systems involved or the particular confidential data that was leaked; rather, the incident arose from strategic and organizational errors.

Desarrollo:

Tradicionalmente la responsabilidad total de administrar la seguridad de la información a recaído en el Departamento de TI, pero las políticas de seguridad de la información o ciberseguridad deben estar estratégicamente alineadas con las metas y objetivos corporativos; no es únicamente una preocupación de TI. El segundo error común es no reconocer la importancia estratégica de la ciberseguridad, al no considerarla crítica para la propia empresa porque “no somos una institución financiera” o "eso es un problema en otros países" o "los objetivos son todas las grandes corporaciones, no empresas de nuestro tamaño". Esta idea errónea lleva a que las empresas presten muy poca atención a la ciberseguridad y subestimen los riesgos que los perpetradores tomarán por sus ganancias ilícitas.

El siguiente factor para considerar es la ausencia de un análisis de riesgo en los activos de información, tanto para inventarios de activos tangibles como los activos de información, el comprender el valor de esos activos y, por lo tanto, evaluar y sopesar los riesgos a los que se encuentran expuestos. La información que posee una empresa es uno de los activos más valiosos; en este caso cada empresa debe saber cuáles son sus activos de información, cómo

clasificarlos, cómo calcular sus riesgos y, por último, cómo protegerlos. Una vez establecida esta evaluación de seguridad de datos debe revisarse periódicamente y ajustarse según lo justifique. La aplicación de una metodología sobre la gestión de riesgos es esencial para garantizar que se identifiquen los activos de información y se midan, evalúen y aborden los riesgos.

Las pequeñas y medianas empresas sufren porque las soluciones de ciberseguridad no están orientadas a su segmento o el hecho de que este segmento suele manifestar poco o ningún interés en la ciberseguridad. Si bien la implementación de una infraestructura segura puede ser costosa, existen varias soluciones tercerizadas que son seguras y económicas y que apoyan a las necesidades de estas empresas. También hay soluciones de computación en la nube que proporcionan seguridad adecuada a un precio asequible. Estas empresas deben buscar el asesoramiento de un consultor con conocimientos no solo en materia de funcionalidad, sino también en seguridad.

Finalmente, también existe una idea errónea muy común en la comunidad de que con la compra de dispositivos se produce un aumento en la seguridad de la información de una empresa, pero este es un gran error. La seguridad de la información en entornos corporativos debe evaluarse desde un punto de vista holístico, comenzando por el eslabón más débil: las personas, para luego realizar una evaluación, que debe analizar las políticas, procesos, procedimientos, arquitectura, hardware, software e infraestructura que conforman el negocio y especificar los niveles de seguridad correspondientes.

Otro detalle relevante es el rompimiento del paradigma de la protección, tradicionalmente se han usado hasta ahora sensores de programas malignos basados en firmas. Los perpetradores, como contramedida, los han modificado para que este pueda “colarse” dentro del flujo “normal” de tráfico con el fin de mimetizarse. Esto ha derivado en un nuevo enfoque del monitoreo y detección, que ahora basa sus sensores en TTP (Técnicas, Tácticas y Procedimientos). El nuevo enfoque se centra en las conductas y actividades, determinando si estamos o no ante actividad maliciosa.

Es tiempo que se analicen las consecuencias económicas, políticas, legales, de reputación e incluso sociales del uso no autorizado o la divulgación de los datos de una empresa y que se reconsidere la estrategia de seguridad de la información y la ciberseguridad corporativa en la toma de decisiones comerciales y/o estratégicas o cuando se desarrollen nuevos procesos para el aseguramiento de toda la información dentro de la empresa.

Referencias bibliográficas

"Panama Papers: Vladimir Putin associates, Jackie Chan identified in unprecedented leak of offshore financial records". ABC News online. April 4, 2016. Archived from the original on April 17, 2016. Retrieved April 18, 2016.

Clark, Nicola (April 5, 2016). "How a Cryptic Message, 'Interested in Data?,' Led to the Panama Papers". The New York Times. ISSN 0362-4331. Archived from the original on August 15, 2016. Retrieved August 12, 2016.

Bilton, Richard (April 4, 2016). "Panama Papers: How a British man, 90, covered for a US millionaire". BBC News. Archived from the original on April 4, 2016. Retrieved April 4, 2016.

"A torrential leak" Archived August 31, 2017, at the Wayback Machine. The Economist. April 9, 2016.

"The Panama Papers: 7 things to know". CNN. April 5, 2016. Archived from the original on April 6, 2016. Retrieved April 5, 2016.

Cyril Bensimon; Christophe Châtelot; Joan Tilouine; Simon Piel (September 15, 2015). "L'encombrant bras droit d'Ali Bongo". LE MONDE (in French).

Sobre el autor:

Luis Gorgona es un profesional con 20 años de experiencia en Tecnologías de Información y 15 años dedicado a la seguridad. Cuenta con la acreditación CISA de ISACA. Durante el periodo 2006-2010 se desempeñó como Director de Seguridad de la Información en La Casa Presidencial de Costa Rica. Durante ese periodo fue instructor en el programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de Estados Americanos (OEA). Desde el 2010, se ha desempeñado como consultor de seguridad de la información para varias empresas.

CyberSecurity
Información & Privacidad

Donaciones

Contraportada
$500.00

Portada Interior
$450.00

Pagina Interior (Especifica)
$400.00

Pagina Interior
$350.00

Media Página
$200.00

Mas Información

info@csecmagazine.com

LINEAMIENTOS PARA LA PUBLICACIÓN DE ARTÍCULOS

I. Lineamientos Generales

Los artículos que se publicarán en la revista Cybersecurity – Información y Privacidad- corresponden a:

• Artículos con los resultados de proyectos de investigación que se hayan llevado a cabo.

• Artículos invitados, solicitados directamente al autor, por el Editor o el Comité Editorial.

• Artículos de síntesis y opinión que unifiquen e interpreten el avance del conocimiento en un tema.

• Ensayos y trabajos.

• Resúmenes y acotaciones sobre conferencias, seminarios, talleres y foros.

• En los números especiales de la Revista, patrocinados por un proyecto, podrán publicarse los artículos en idioma inglés.

Las cuales deberán atender los siguientes lineamientos:

1. Deben exhibir coherencia conceptual, profundidad en el dominio de la problemática abordada.

2. Estar escritos en un estilo claro, ágil y estructurado de acuerdo con la naturaleza del texto; con base al modelo APA 6ta. Ed.

3. La extensión mínima del artículo será de 2 páginas con un máximo de 10, formato Word, letra tamaño 12, tipo Times New Roman, interlineado 1.5, márgenes de 3 centímetros, hoja tamaño carta.

4. Los artículos deberán ser entregados en formato digital al correo de la asistente de editores cfa@csecmagazine.com

5. Presentar carta firmada por el autor, según formato anexo, indicar la cobertura temática del artículo de acuerdo con la clasificación según la especialidad.

6. Los manuscritos para su publicación deben incluir:

Título. Debe escribirlo en mayúscula y negrilla, no contener fórmulas ni abreviaturas, ser breve y consistente con el trabajo. En idioma español y en inglés.

Nombre de los autores. Se escribe el primer nombre, la inicial del segundo nombre si lo hay, seguido del apellido. Cuando existe más de un autor, se separan con comas. Se debe indicar con un asterisco la persona a la que puede dirigirse la correspondencia. Además de un extracto del resumen de su experiencia laboral, profesional, adicionando una foto de estudio a color, correo electrónico y redes sociales (LinkedIn)

Nombre de la institución y dirección. Para indicar la afiliación de cada autor use superíndices en el nombre del autor. Para el autor que lleva el asterisco se debe indicar, la dirección completa, teléfono, fax y correo electrónico, a donde pueda dirigirle la correspondencia. Esto solo aplica si representa a una empresa y ha establecido un contrato de publicidad en la revista.

Resumen en español. No debe exceder de 250 palabras. Debe contener los principales resultados y conclusiones haciendo énfasis en los logros alcanzados. Como los resúmenes son copiados directamente de las bases de datos por los interesados, deben contener en forma abreviada el propósito del estudio y las técnicas experimentales, los resultados e interpretaciones de los datos. Los términos relevantes importantes para comprender el contenido del artículo. Se debe entender con facilidad sin tener que recurrir al texto completo.

Introducción. No es necesario incluir toda la literatura sobre el tema en esta sección. Se debe describir el planteamiento general, con la información necesaria en forma concisa, haciendo referencia a los artículos directamente relacionados y que se considere indispensable para el desarrollo del tema y que permita al lector encontrar a otros investigadores del campo, relacionados con el problema o interrogante planteada por el autor. No se deben, por lo tanto, incluir revisiones amplias de la bibliografía.

Materiales y métodos (Opcional): Si existen secciones diferenciadas, deben indicarse con encabezados pertinentes (por ejemplo, síntesis, muestreo, preparación de muestras, etc.). La explicación de los métodos experimentales debe hacerse con los suficientes detalles para que otros investigadores puedan repetirla. La descripción de equipos y reactivos sólo se debe incluir cuando sean específicos o novedosos. Se debe evitar la descripción de procedimientos aplicados con anterioridad por otros autores, pero se debe citar la bibliografía pertinente. Si existen modificaciones a procedimientos ya publicados, se deben incluir los detalles de esta.

Resultados de discusión (Opcional). Presente los resultados en forma clara y concisa, en lo posible en uno de los siguientes formatos: texto, tablas o figuras. Evite duplicar la presentación de los resultados en tablas y figuras. La discusión debe proporcionar una interpretación de los resultados en relación con trabajos previamente publicados y no debe contener repetición considerable o amplia de la sección de resultados o reiteración de lo dicho en la introducción. La información escrita en el texto debe ser citada, pero no se debe repetir en detalle lo ya expuesto. En la discusión es permitida la especulación, pero debe estar bien fundamentada. Dedique al final un párrafo para hacer resaltar las conclusiones más relevantes del trabajo.

Bibliografía. Listado de las fuentes bibliográficas citadas en el artículo en orden alfabético, según el apellido del primer autor, utilizar el modelo APA 6ta. Ed.

POR MOTIVOS DE DERECHOS DE AUTOR, ARTICULOS PUBLICADOS EN OTRAS PLATAFORMAS NO SE TOMARÁN EN CUENTA PARA EVITAR TEMAS LEGALES, A MENOS QUE EL AUTOR INDIQUE CLARAMENTE QUE ES PROPIETARIO DE DICHA INVESTIGACION.

La Editorial

cfa@csecmagazine.com

Ciudad , mes de 2,0.

A:

Coordinadora de la Revista Cybersecurity

Presente.

Yo, _____de nacionalidad _____

Identificación No. _____

correo electrónico_____: Teléfono: _____,

Hago constar que el artículo con título:

Acerca de una investigación con el nombre:

Que presento es original y nunca ha sido publicado en otra revista, medio escrito o electrónico y tampoco ha sido presentado a arbitraje en otra revista impresa o digital.

Además, acepto las normas de la revista, en cuanto a procedimiento, formato y demás procedimientos indicados en los lineamientos para publicación de artículos.

_____

Firma

Magazine
CyberSecurity
Información & Privacidad

AUCI invita a participar en la

Convocatoria de Artículos de Ciberseguridad en la

Revista Digital Cybersecurity – Información & Privacidad

(CFA)

Si eres investigador y/o tienes un artículo sobre ciberseguridad de tu autoría, envíanos tu resumen para poder analizarlo y posteriormente publicarlo.

cfa@csecmagazine.com

Magazine

CyberSecurity

Información & Privacidad