CIBERSEGURIDAD EN DEFENSA DE SU EMPRESA DESPROTEGIDA

Lilián Angeles Espinoza
langelese1602@alumno.ipn.mx
Edwin Uriel De Santiago Landeros
edesantiagol1600@alumno.ipn.mx
Vicario Solorzano Claudia Marina
cvicario@ipn.mx

Instituto Politécnico Nacional
Unidad Profesional Interdisciplinaria de Ingeniería
y Ciencias Sociales y Administrativas

Boletín No. 90
1o. de mayo de 2022

Resumen

La ciberseguridad es el conjunto de elementos, medidas y equipos destinados a controlar la seguridad informática de una entidad o espacio virtual, es elemental contar con esta, debido a los diversos ciberataques que han llegado a demostrar las vulnerabilidades de las empresas, gracias a los análisis de riesgo de seguridad informática se puede implementar en los distintos campos de la industria del software se es necesario la implementación de una metodología para proceso de ciberseguridad, este proceso nos muestras minuciosamente los pasos por los que ejecuta, Cabe recalcar, que el nombre que recibe esta implementación de reglas, se le conoce como normas ISO que se clasifican en 3 fases, para una mejor optimización en las organizaciones ya que deben ampararse en las distintas medidas que ofrece la ciberseguridad por lo que existe el Centro de Innovación en Inteligencia y Seguridad (CIIS), el cual usando los conocimientos científicos y de vanguardia interviene con estrategias innovadoras en México y el resto del mundo. Este último año se ha registrado con la pandemia una aceleración de los programas de digitalización de las compañías, adelantado así sus planes entre dos y tres años, de manera que la información de la empresa debe de estar protegida. Cabe aclarar que la ciberseguridad se desarrolla por fases lo que hace a cada una importante y a su vez necesaria dependiendo de la situación de la empresa. Pero ¿cuáles son los peligros del cual nos tenemos que proteger?, en realidad la lista es muy larga, pero mencionaremos los más comunes y peligrosos que utilizan los ciberdelincuentes. Pero ya que nada es impenetrable, nombraremos los errores que pueden llegar a existir en los sistemas de ciberseguridad, que suelen ocasionar algunos errores, al momento de ejecutarlos.

Palabras Clave: vulnerabilidades, ciber-ataques, normas ISO.

Abstract

Cybersecurity is the set of elements, measures and equipment intended to control security information and entity or virtual space, it is essential to have this, due to the various cyber-attacks that have come to demonstrate the vulnerabilities of companies. Thanks for the risk análisis of computing security can implement in the various fields

the software industry is necessary the implementing the methodology of the cyber security process, this process shows the implementation of rules, it is known as ISO standards, which are classified into 3 phases, for better optimization in organizations since they must take advantage of the different measures offered by cybersecurity, for which there is the Innovation Center in Intelligence and Security (CIIS), which uses scientific and cutting-edge knowledge intervenes with innovative strategies in Mexico and the rest of the world.
This last year, the pandemic has caused an acceleration in the digitization programs of companies, thus advancing their plans by two to three years, so that company information must be protected.
Cybersecurity is developed in phases, which makes each one important and in turn necessary depending on the situation of the company. But what are the dangers from which we have to protect ourselves? Actually the list is very long, but we will mention the most common and dangerous ones used by cyber criminals. But since nothing is impenetrable, we will name the errors that may exist in cybersecurity systems, which usually cause some errors, when they are executed.

Keywords: Vulnerabilities, cyber-attacks, ISO standards.

I. Introducción

Desde un punto de vista y pensamientos del avance tecnológico en México, podemos visualizar que es el segundo país que cuenta con una inmensa variedad de empresas que han sufrido ciberataques, mostrando principalmente pérdida de datos de servidores, pérdida de productividad, perdidas de robo de identidades, como ejemplo algunos de los sectores que fueron punto de mira para estos ataques son instituciones financieras, sistemas de infraestructura crítica, industria 4.0, cadenas de suministro...etc. Pero ¿qué ha hecho que sea uno de los principales países en tener este tipo de problemas?, como respuesta a ello podemos decir que la falta de implementación en las distintas metodologías que podemos encontrar en el campo de la ciberseguridad, tomaremos como ejemplo la norma ISO/IEC 27032 que guía a este ámbito y se centra en dos áreas; ser proactivo en las normas de seguridad y en aplicaciones de prevención. Pero también debemos enfatizar en sitios que son más vulnerables para estos ciberdelincuentes, ya sea desde páginas web, aplicaciones, inclusivamente en los portales web de empresas de alto nivel, todo esto ha crecido de una manera colosal, principalmente por el actual tema de salud del SARS-CoV-2 (Coronavirus), las empresas se han visto afectadas.

"Al no poder operar normalmente, las organizaciones deben apoyarse en sus empleados vía trabajo remoto, pero tienen que observar políticas de seguridad. Por ello, deben contar con antivirus y antispyware, además de sistemas actualizados, sin excepción" (Fernando Thompson 2015), director general de tecnologías de la Información de la Universidad de las Américas Puebla (UDLAP), entre los ataques más frecuente: son crypto hacking (10 %), exposición de datos internos (28 %), ransomware (25 %), robo de credenciales (19 %) y malware (34 %). De esta manera, México está en el décimo primer lugar a nivel mundial con más casos de ataques, siendo la India el primer lugar con el 93 % de las organizaciones afectadas en el último año. Debido a esto podemos deducir que hay más ataques hacia empresas que a usuarios comunes, como un gran factor de riesgo y con el propósito de generar soluciones viables la institución CIIC decidió capacitar y promover la importancia del conocimiento de ciberseguridad industrial, gestión de la seguridad a la información, análisis de vulnerabilidades…etc. para poder cesar a estos ataques y de esta manera, puedan estar más preparados y menos vulnerables. Cabe aclarar que esta institución está a nivel mundial, pero en este artículo nos basaremos en ciberataques hacia México. Cabe recalcar que las herramientas, cursos y consejos que mencionaremos, pueden tener vulnerabilidades, todo esto lo mencionaremos a continuación.

II. Los ciberataques no son cosas de ciencia ficción

A lo largo de la historia, los problemas y ataques hacia empresas se han visto presentes y aunque han sido diferentes las maneras de atacar tomamos, como factor principal la tecnología que va evolucionando para mejorar la calidad y facilitar los distintos sectores de empresas públicas y privadas. Sin embargo, esto también puede ser de mal uso ya que ha sido un avance hacia grandes ataques cibernéticos, pero al ser una nueva era de avance tecnológico, las empresas se ven vulnerables por la ignorancia de estos temas, debido a la falta de capacitación; sin importar cual sea el factor es necesario tomar en cuenta que en México, podemos encontrar un gran sector de microempresas y

macroempresas, las cuales pueden sufrir un gran riesgo de ciberataques “El 30 % de las empresas de América Latina aseguran haber sido víctimas de un ciberataque en el último año, de las cuales el 45 % hace referencia a la pérdida de reputación como la consecuencia más frecuente y directa de estos ataques. Un 41 % de los encuestados, consideran que el desconocimiento y el error humano son las principales causas de los incidentes de seguridad informática en sus compañías” Ámbito Financiero; [Buenos Aires] (2020), los principales sectores en riesgo son:

1. Sistemas de infraestructura: “entre ella de corriente eléctrica, suministro de agua, sistemas de transporte, fuerzas de seguridad y servicios de emergencia. En las empresas, los sistemas hacen posible la operación y expansión del negocio. Un ciberataque a este sector es el ataque contra Pemex cuando en noviembre de 2019 la paraestatal sufrió un ataque a su infraestructura crítica con ransomwere (secuestro de datos). Las consecuencias son principalmente la interrupción de las operaciones que puede ocasionar pérdidas económicas cuantiosas, poner en peligro la vida humana o dañar al medio ambiente”
2. Instituciones financieras: “Donde más de 40 % de estos intentos de ataques tuvieron éxito. Tanto como bancos Fintechs, Sociedades Cooperativas de Ahorro y Préstamos (Socaps) y Sociedades Financieras Populares (Sofipos) fueron víctimas de ataques cibernéticos que les costaron durante el 2018 alrededor de 107 millones de dólares en respuestas y recuperación”
3. Cadena de suministro: “Es un conjunto de elementos que permiten que las empresas cuenten con la organización necesaria para llevar a cabo el desarrollo de un producto o servicio. Los ciberataques tienen como objetivo vulnerar los sistemas de los equipos y maquinaria provistos por terceros proveedores de una empresa para luego introducir malware que afecte a otros sistemas de la organización”
4. Industria 4.0: “Este concepto se refiere a una nueva fase en la Revolución Industrial que se enfoca en la interconectividad, automatización, aprendizaje automatizado y los datos en tiempo real. Así, las empresas integran la producción y las operaciones físicas con tecnología digital inteligente, aprendizaje automatizado y big data para crear un ecosistema más conectado.”

No debemos olvidar que no solo las empresas, pueden recibir ataques cibernéticos “los vectores de ataque más comunes de Phishing son dos: Por Spoof Email, y por Spoof Website. Phishing Email es la técnica preferida por los Phishers, debido a que, por medio de un simple spam, se les pide a los usuarios que envíen información privilegiada. Por su parte, Spoof Website hace referencia a una página web cuya apariencia es una copia de una página web original, en la que igualmente se induce a que él usuario ingrese información sensible” A. N. Shaikh, A. M. Shabut, and M. A. Hossain (2016).

1. Auditoría interna en los procesos de las áreas de Redes, Desarrollo de Software y Documentación: La auditoría interna se realiza con la finalidad de llevar un control de los procesos que se llevan a cabo en las diferentes áreas de una organización, y a la vez verificar que el cumplimiento de estas actividades se efectúe de acuerdo a regularizaciones formales nacionales (normativas, manuales, procedimientos) e internacionales (estándares, marcos de control, buenas prácticas). El formato aplicado para esta auditoría está basado en la ISO/IEC 27032 directrices de Ciberseguridad bajo los dominios de seguridad de Redes, Información y Aplicaciones para los sistemas distribuidos. se observa un formato de checklist aplicable para la auditoría interna, para este caso, se puede utilizar para evaluar toda la documentación que se lleva a cabo en los procesos de seguridad de la información, así como en las aplicaciones y en las redes, por lo tanto, se elabora un checklist para cada dominio con la que trabaja la norma ISO/IEC 27032.
2. Análisis de Vulnerabilidades: se procede a clasificar la información obtenida de acuerdo con la ponderación e identificación del estado de los procesos en documentación efectuada en el checklist. El resultado de la valoración serán las vulnerabilidades encontradas en los sistemas distribuidos. El análisis de las mismas corresponde a la evidencia suscitada en la solicitud de información al momento de aplicar el checklist, y de acuerdo al estado de vulnerabilidad se realiza el siguiente cuadro para su clasificación, Con la obtención de los datos se puede realizar una comparativa con los resultados obtenidos en los diferentes dominios de la norma ISO/IEC 27032, y con ello determinar la ubicación de los fallos en la parte técnica de los sistemas distribuidos.
3. Identificación de Riesgos: Para la comprensión de los riesgos que podrían tener estas vulnerabilidades en los sistemas distribuidos, se pueden utilizar metodologías de gestión de riesgos como la ISO/IEC 27005, AMFE (Análisis Modal de Fallos y Efectos) y herramientas de cómo Marisma. Para este estudio se consideró la AMFE por su precisión en la identificación y

priorización de los riesgos en las vulnerabilidades encontradas en los sistemas distribuidos de la empresa. La implementación fue aplicado al cumplimiento de la Norma ISO 27032 cubriendo los dominios de Seguridad de la Información, Seguridad en las Aplicaciones y Seguridad de Redes.

Como paso primordial debemos mencionar que los pasos mencionados, pueden ser de gran utilidad para la implementación de esta metodología, ya que cuenta como primordialmente el análisis de las vulnerabilidades de sus sistemas, para que puedan encontrar distintos factores de riesgo. “La investigación realizada por Hyunguk y Taeshik (2015), menciona que, de acuerdo con la revisión, no se tienen estudios sobre los tipos de nuevas vulnerabilidades de seguridad y los requisitos de seguridad que se requieren en un entorno de protocolo heterogéneo basado en IEC 61850” Hyunguk y Taeshik (2015).

IV. ¿Qué tan vulnerable es tu sistema?

Como lo hemos visto las empresas son principalmente las que corren mayor riesgo, sus sistemas son los que fallan y por ello pueden tener vulnerabilidades graves, de acuerdo con el informe realizado se analizó a 45,000 sitios web y red escaneos realizados. Desde abril de 2015 hasta marzo de 2016, mas de 5,700 objetos escaneados mostro que el 60 % de los sitios web registraban vulnerabilidad de gravedad alta y se encontró que el 74 % de las aplicaciones de internet tenían vulnerabilidades de gravedad media. “El 94 % de las ciber amenazas provienen del correo electrónico y en perspectiva, los ataques al correo electrónico representaron un estimado de 1,770 millones de dólares en pérdidas para las organizaciones en 2019”. (Darktrace, empresa líder mundial en la tecnología Enterprise Immune System para ciberseguridad, 2020).

V. Covid-19; EL nuevo virus que afecta a las empresas

Como bien sabemos, el nuevo virus Covid-19 ha afectado a cada rincón del planeta, cada ser humano, pero víctima de ello las empresas. Por lo que ellas son las que más responsabilidad tienen, ya sea para proceso, producción e implementación de servicios que se usan día a día, como consecuencia primordial debemos mencionar que han tenido que poner en práctica un nuevo modo de trabajo hacia sus empleados para un trabajo a larga distancia, implementado sistemas que como bien pueden ser útiles, Çreemos que se trata de una cobertura cada vez más importante, tanto para empresas como particulares, por el fuerte incremento del trabajo remoto, el auge de las redes sociales y un menor nivel de seguridad debido al home office, pero el mercado local todavía no incorporó ésta cobertura en forma generalizada”Gonzalo Ketelhohn (2020), también corren riesgo por falta de información y experiencia de estas, como consecuencia de ello muchas empresas han sido víctimas de ciberataques enfrentado grandes problemas y pérdidas de bienes de las empresas. “El riesgo principal que vemos para 2021 seguirán siendo los usuarios. La transformación digital ya se venía dando, pero la pandemia obligó a las organizaciones a volverse productivos digitalmente y tal vez se dejaron de lado las cuestiones de seguridad”. (Ramón Castillo, 2020).

VI. ¿Qué ataques puedo recibir?

Son variados aquellos ataques que son muy comunes de escuchar que son los causantes de esas puertas traseras a los sistemas y de los cuales debemos de cuidarnos entre ellos son:

1. Malware: Hace referencia a cualquier programa o código informático dañino que tiene la capacidad de afectar el correcto funcionamiento en un sistema, de manera parcial.
2. Ransomware: Programa de software malicioso que infecta tu computadora y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema.
3. Cryptojacking: Implica una amenaza continua proveniente de Internet que se mantiene oculta en un ordenador o dispositivo móvil, por medio de los
4. Recursos del equipo extrae monedas digitales tal es el caso de las criptomonedas. Esta amenaza es capaz de apoderarse de navegadores web, y a su vez diversos dispositivos e incluso servidores de red.
5. Spyware: Es una aplicación que compila información sin el consentimiento del usuario, con el objetivo de vender esta información a empresas publicitarias u otras organizaciones interesadas. comúnmente, este software envía información a sus servidores, de acuerdo con los datos de navegación del usuario, además obtienen la información que se solicita en esos sitios, así como direcciones IP y URL. Se considera el origen otra plaga como el SPAM.
6. Rogue: Se trata de un programa falso que pretende ser algo que no es. Esto surgió desde “Falsos Optimizadores” de Windows, y “Falsos Antivirus” lo cuales han evolucionado. Al momento de

que el usuario lo ejecuta muestra una falsa infección o problema en el sistema, entonces este programa pretende arreglarlo, por lo cual pide al usuario comprar el software falso, lo cual es simplemente una gran estafa.
7. Phising: Consiste en el robo de información individual y/o especulador del usuario, mediante la falsificación de una entidad de confianza. De manera que el usuario cree compartir su información con un ser de confianza cuando, en realidad, está brindando estos datos a su atacante.
8. Keylogger: Softwares que tienen la función de almacenar en un archivo toda la información que el usuario ingrese desde el teclado. Usualmente, pretender robar contraseñas e información del dispositivo en el que se ha instalado la aplicación.

Como podemos ver son bastantes los riesgos que puede llegar a tener las empresas si no se llega a preparar de una mejor forma. “los sistemas informáticos están sometidos a potenciales amenazas de seguridad de diversa índole, originadas tanto desde dentro de la propia organización, como desde fuera, procedentes de una amplia variedad de fuentes. A los riesgos físicos, entre ellos, accesos no autorizados a la información, catástrofes naturales, sabotajes, incendios, y accidentes; hay que sumarle los riesgos lógicos como contaminación con programas malignos, ataques de denegación de servicio y otros. Fuentes de daños como códigos maliciosos y ataques de intrusión o de denegación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados” (Oficina de Seguridad para las Redes Informáticas, 2018).

VII. CIIC

México al ser uno de los primeros países que recibió más ciberataques a sus empresas, durante los últimos años ha implementado medidas drásticas, “A nivel institucional, en México se observa un importante incremento presupuestal, que se le ha asignado a proyectos relacionados con seguridad cibernética y temas de capacitación en esta área, debido al incremento en 2018, con más del 70 por ciento de las organizaciones incrementaron sus presupuestos relacionados a invertir para temas de ciberseguridad” Arnulfo Espinoza (2018). Una de las principales implementaciones es el Centro de Innovación de Inteligencia que se encarga de contribuir en el desarrollo de personal calificado, para implementar y capacitar las empresas con sus múltiples cursos y servicios de Consultoría, Educación Continua, así como certificación de planes y proyectos. Gracias a que cuenta con cursos, la plataforma en donde puedes encontrar los diferentes servicios muestra una gran variedad de cursos, lo mejor de esto es que te presenta una pequeña introducción del tema que será visto y quién lo impartirá, además de tener disponibilidad de horarios y distintas categorías como lo son:

1. Ciber-ataque
2. Ciberseguridad
3. Cursos y capacitaciones
4. Educación
5. Exploits
6. General
7. Ingenieria Social
8. Malware
9. Phising

A medida que entra a la categoría que sea de tu interés se van desplegando sub categorías así como programas de actualización en ciberseguridad, desde cibercriminalidad, ataques BadUSB, peligro en los ataques MITM (Man-in-the.middle), ramsoware, detección de virus, seguridad IA. Con esta gran variedad de temas y facilidades que te ofrece el Centro de Innovación en Inteligencia y Seguridad, ninguna empresa debería de estar desprotegida. Como parte de la educación se ha tomado una gran medida programas en seguridad, diplomados en administración y operación de la seguridad con el fin de obtener personal altamente capacitado, además de tener un equipo de profesionales en las distintas categorías ya mencionadas cuyo conocimiento y experiencia garantiza su calidad en los servicios.

VIII. ¿100 % Seguro?

Como bien sabemos nada es 100 % seguro, pero por ello mismos se toman medidas, perspectivas hacia una mejor resolución si llegara a tener problemas, pero son muchos los factores que se deben de tomar para saber los errores y puedan manejar una resolución más eficiente, entre ellas están:

1. Diseño de seguridad perimetral.
2. Debilidad en el diseño de protocolos utilizados en las redes.
3. Políticas de seguridad deficientes e inexistentes.
4. Errores de programación.
5. Existencia de "puertas traseras" en los sistemas informáticos.
6. Uso
7. Configuración inadecuada de los sistemas informáticos.
8. Desconocimiento de los usuarios y de los responsables de informática.

Es primordial que, al hacer todos los análisis, implementación de metodologías y precauciones, se recomienda dar revisiones continuas y no dejar pasar un gran lapso de revisión.

Conclusión

Referente a la educación y el ámbito empresarial llegamos a un argumento importante que es esencial a mencionar respecto a nuestro país, recordemos que en los últimos años se ha recibido más de 1000 ataques a servidores de empresas, que como se argumentó en el contenido de este artículo es un gran problema para la industria informática, con base en lo anteriormente relacionado creemos que tienen objetivos bien centrados para la solución y desarrollo de software de ciberseguridad.

Cabe recalcar que la ciberseguridad es primordial en una empresa, debido a la gran cantidad de información con la que trabaja; es importante prevenir los ciberataques, además de actualizarse en dicho tema, para evitar la exposición de información innecesaria.

De otra forma, podemos asumir que gracias a las varias organizaciones principalmente al CIIC que proporciona de manera detallada los temas que se relacionan con ciberataques en relación con la ciberseguridad.

Finalmente, esperando disminuir el crecimiento exponencial de los ciberataques con la información brindada y recaudada actual.

Referencias

1. Fernando Thompson (**2015**). *director general de tecnologías de la Información de la Universidad de las Américas Puebla (UDLAP)*de https://esemanal.mx/2020/05/pronostican-40-mas-de-ataques-ciberneticos/

2. A. N. Shaikh, A. M. Shabut, and M. A. Hossain (**2016**). *A literatura review on phishing crime, prevention review and investigation of gapsin 2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)*2016, pp. 9–15 de https://search.proquest.com/docview/2474916627/fulltextPDF/D37AF409237443BPQ/1

3. Espinel-Ortega., A., y Carreño-Perez., J.C. (**2020**). *Identificación de activos y ciberactivos críticos en sistemas de transmisión de energía eléctrica.* Tecnura, 24(65)27-38 Recuperado de https://search.proquest.com/docview/2462465752/fulltextPDF/A742043474714EDEPQ/1

4. Notimex (**2018**). *Empresas aumentan presupuestos para proyectos de seguridad* de https://search.proquest.com/docview/2047364728/5DECDFF4C94C49A6PQ/9

5. Andrea Rivas (**2020**). *Gonzalo Ketel hohn: "Creemos que la cobertura frente a ciberataques tendrá un salto en 2021"*en https://search.proquest.com/docview/2472007156/5DECDFF4C94C49A6PQ/18

6. Ambito Financiero; Buenos Aires [Buenos Aires] (**08 Dec 2020.**). *¿Por qué es importante construir una empresa ciber-resiliente?* https://search.proquest.com/docview/2469021960/5DECDFF4C94C49A6PQ/21

7. Chavez, Gabriela (**2020**). *El home office sienta las bases para actualizar la Ley de Protección de datos*extraído de https://search.proquest.com/docview/2469399991/5DECDFF4C94C49A6PQ/92

8. David Basin (**2016**). *Muchos profesionales de la informática afirman que estamos entrando en una nueva ola de innovación tecnológica que se ha denominado Ïnternet de todo.º IOE. Una característica principal de la IOE es una conectividad avanzada de dispositivos, sistemas y servicios que podría conducir a más violaciones de seguridad. ¿Cuáles son algunas áreas prometedoras de investigación en seguridad de la información que podrían mantener la seguridad y permitir un grado mucho mayor de conectividad?* ? https://www.acm.org/articles/people-of-acm/2016/david-basin

9. Reyes, Eréndira (**2020**). *Estas fueron las lecciones de ciberseguridad que nos dejó el 2020* https://search.proquest.com/docview/2471143807/6880104293DF48D1PQ/7

10. Carrillo, Jessica Johanna Morales (**2020**). *Proceso de Ciberseguridad: Guía Metodológica para su implementación*implementación https://search.proquest.com/docview/2394538125/EA092B75A3494358PQ/2