"Seguridad en el ecosistema digital: ciberseguridad, ciberespacio y las personas"

Ing. Santiago Trigo[1], Ing. Gonzalo Ruíz De Ángeli[2], Lic. Sandra Cirimelo[3]
Universidad FASTA, Facultad de Ingeniería
[1]:santiagotrigo@ufasta.edu.ar
[2]:ruizgon@ufasta.edu.ar
[3]: scirimelo@ufasta.edu.ar

Resumen

Cada vez son más las amenazas que existen en el mundo digital, por lo que resulta indispensable utilizar y gestionar la tecnología en forma segura y con responsabilidad. A diario, ocurren ciberataques de tipos variados y con objetivos diferentes. Dichos ataques pueden realizarse "desde afuera" o "desde adentro". Por la complejidad y baja efectividad relativa de los primeros, los ciberdelincuentes eligen la segunda alternativa, cada vez con mayor frecuencia. Para poder llevar adelante este tipo de ataques, los delincuentes se basan en la manipulación de las personas, a través de la ingeniería social, para poder acceder a los sistemas o introducir un malware en la red. Esto hace evidente desde hace un tiempo, que las personas tienen un rol clave cuando se habla de ciberseguridad, motivo por el cual se deben desarrollar con mayor urgencia y con la importancia que se merece, políticas organizacionales de ciberseguridad en ámbitos públicos o privados y en cualquier tipo de institución: empresas, entidades educativas, gubernamentales, entre otras. Además, resulta fundamental una mayor concientización de las personas y mayor capacitación para contar con más y mejores profesionales en la materia.

Introducción

El mundo ya es definitivamente digital y no hay posibilidad de retroceso en este sentido. Por el contrario, el desarrollo de tecnologías como Virtualización, Inteligencia Artificial, Ciencia de Datos y Big Data, Internet de las Cosas (IoT), Computación en la nube, Realidad Aumentada, Nanotecnología, Robótica autónoma, Simulación virtual computarizada, Blockchain, Criptomonedas, etc. ya está entre nosotros y las organizaciones descansan en ellas.
El ciberespacio es el ambiente complejo que resulta de la interacción de personas, software, y servicios en internet por medio de dispositivos y redes conectadas. No posee existencia física, sino que es un dominio virtual que engloba todos los sistemas TICs[1]. Es un dominio muy complejo. Allí se desarrollan actividades de creación, procesamiento, almacenamiento, intercambio y visualización de información usando software y hardware interconectado. Lo constituyen tanto Internet como todas aquellas redes aisladas que se utilizan con finalidades particulares.
En este mundo digital interconectado donde todos, personas y dispositivos, producen información en cada instante, el volumen de la misma crece geométricamente y su administración es cada vez más compleja, aparece, entonces, una dimensión de riesgos que ponen en jaque a las organizaciones en general donde no todas, están preparadas para enfrentarlos.

[1] JEFATURA DE GABINETE DE MINISTROS. SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN. Resolución 1523/2019. Anexo II - Glosario de Términos de Ciberseguridad.

Cada vez son más las amenazas que existen en el mundo digital y cada vez, entonces, es más necesario utilizar y gestionar la tecnología en forma segura y con responsabilidad, desde los escenarios más complejos como instalaciones críticas digitales, de producción y servicios hasta los dispositivos aparentemente inofensivos y generalmente no administrados como un celular, un reloj inteligente, un electrodoméstico o un sensor que se vincula con cientos de sistemas informáticos y otros dispositivos. La frecuencia de los ataques, como el Ransomware o el Phishing, pone en verdadero riesgo a todo tipo de organizaciones. Muchos de estos delitos informáticos, entendidos, según Sain (2021), como *"todas aquellas conductas antijurídicas, ilícitas o ilegales que vulneran derechos o libertades de las personas y utilizan un dispositivo informático como medio para la comisión del mismo, o el mismo es el fin del delito.",* ocurren o pueden ocurrir debido a fallas o incidentes de seguridad informática y requieren no sólo de la gestión activa de la seguridad sino del estudio del fenómeno para poder prevenirlos y combatirlos y la concurrencia de la informática forense para la investigación ex post de lo ocurrido ante cada incidente.

La ciberseguridad se encarga de la preservación de la confidencialidad, integridad, disponibilidad y autenticidad de la información en el ciberespacio[2], poniendo el eje en la seguridad de las personas, de los ciudadanos. Además, contempla la problemática de los delitos informáticos (diferente a los incidentes de seguridad informática) donde, por ejemplo, la ingeniería social puede dar lugar a ellos, sin que conformen un problema de seguridad informática. La ciberseguridad no se reduce a una cuestión técnica de la informática, ni es sinónimo de "seguridad informática". En concreto, la gran mayoría de las denuncias de delitos que se producen en el ciberespacio en la actualidad tienen que ver con la seguridad de las personas.

En la investigación de estos delitos informáticos aparecen cuestiones de la criminalística y del derecho que son imprescindibles tenerlos en cuenta. En la prevención, incluso, aparecen cuestiones de la psicología y sociología que considerar. Todos estos aspectos hacen a la ciberseguridad y nada tienen que ver con la seguridad informática, aunque la seguridad informática pueda ayudar a prevenirlos y la informática forense pueda ayudar a esclarecerlos. Cuestiones tan elementales como la educación o concientización de las personas de una organización (y de ciudadanos en general) sobre los riesgos y cómo "cuidarse" en el ciberespacio hacen a la ciberseguridad y no son cuestiones de la seguridad informática. Claramente, la ciberseguridad va más allá de la informática y no es una cuestión de ingenieros, aunque éstos sean partícipes fundamentales, junto a otros profesionales. Una política de ciberseguridad, en síntesis, es una política criminológica, que recurre en algunos aspectos a la informática en general y en algunos temas puntuales a la seguridad informática o informática forense como instrumentos.

Desarrollo

El sector público no es ajeno a recibir ataques informáticos. Por el contrario, se han convertido últimamente en un objetivo primordial de los delincuentes. No es necesario hacer mención a casos específicos, pero son de público conocimiento los ataques recibidos a los tres poderes del Estado ya sean a nivel municipal, provincial o nacional como así también a los diferentes Ministerios de cada uno de ellos. Es decir, toda la organización pública se ve afectada por este tipo de eventos adversos. Lo cual, es

[2] JEFATURA DE GABINETE DE MINISTROS. SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN. Resolución 1523/2019. Anexo II - Glosario de Términos de Ciberseguridad.

lógico. Si partimos de la base que cualquier servicio que sea expuesto a Internet va a ser objeto, en mayor o menor grado, de un intento de ataque, no debe por qué asombrar tal situación. Ahora bien ¿está el sector público preparado para hacer frente a este tipo de situación? ¿el sector público cuenta con las herramientas, humanas y técnicas, para prevenir y actuar frente a los diferentes tipos de ataques que puedan suscitarse en el mundo digital? Las respuestas a estas preguntas, son las que deberían hacerse a la hora de hablar de ciberseguridad e implementar políticas al respecto.

Los ataques informáticos hacia una organización pueden provenir de dos formas diferentes, como muestra la Figura 1.1:

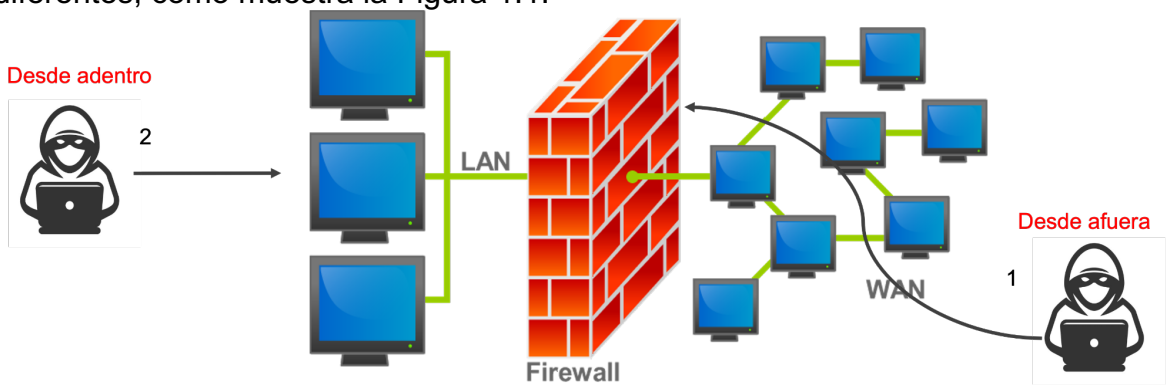

Figura 1.1: Formas de ataque. Elaboración propia.

Los ataques *"desde afuera"* corresponden a las formas que tienen los cibercriminales de vulnerar los sistemas. Es un tipo de ataque sobre los dispositivos y aplicaciones que están siendo ejecutadas sobre ellas. Así se pueden describir algunas metodologías de este tipo de intrusiones, tales como:

- **Vulnerabilidades sobre las aplicaciones o sistemas:** puede corresponderse a fallas, conocidas o no, que permitan la ejecución de algún tipo de malware[3] que permita, entre otras cosas, la intrusión remota al sistema.
- **Claves por defecto:** exposición de sistema o aplicaciones con las credenciales de acceso al mismo dejadas de fábrica o muy sencillas de adivinar.
- **Exposición de datos sensibles:** en muchas ocasiones, no se controla qué es lo que se expone a Internet, dejando información sensible a la vista de cualquier persona. Un delincuente podría usarla para redirigir o utilizar esa información para cometer algún delito.
- **Exposición de servicios sin control:** en ocasiones se exponen a Internet servicios que no deberían estar de esa forma sin ningún tipo de control o enmascaramiento. Un ejemplo claro puede ser el escritorio remoto, precisamente el servicio de Microsoft Windows, cuyas siglas son RDP. Los delincuentes pueden intentar realizar fuerza bruta o ataque por diccionarios[4] a este servicio para lograr acceder a los mismos con claves de administrador, por ejemplo. Una vez dentro del sistema, pueden realizar diversas acciones como ejecutar algún tipo de malware o robar información sensible.

Ahora bien, al hablar en términos económicos, el costo/beneficio que podría incidir en este tipo de intrusión, podría ser bastante alto. En primer lugar, se requieren ciertas

[3] Malware: software malintencionado cuyo objetivo es atacar a la disponibilidad, integridad, confidencialidad o autenticidad.
[4] Kaspersky: https://latam.kaspersky.com/resource-center/definitions/brute-force-attack

características técnicas del delincuente para poder explotar este modo de ataque. En segundo lugar, las probabilidades de un ataque exitoso pueden ser bastante bajas ya que dependerá, siempre, de los controles de seguridad con los que cuente la organización que está siendo objeto del ataque.

Para subsanar estas desventajas que presenta un ataque "desde afuera", aparece una modalidad, que es la más utilizada por los delincuentes, y se la puede denominar el ataque o intrusión *"desde adentro"*. Es decir, en esta situación, no se ataca al dispositivo, aplicación o sistema, se ataca a la persona que ya está dentro de la organización. Entonces las trabas de los controles de seguridad que imponga una organización, no tienen incidencia ya que, una vez vulnerada la persona, directamente ya el delincuente se encuentra dentro de la organización o bien, robó la información que necesita y que fue la misma persona o usuario, con acceso a esa información, quien se la brindó. Se reduce la *expertise* necesaria del delincuente para vulnerar un sistema y se saltean los controles de seguridad impuestos por la organización. Ya no se necesita un delincuente experto en informática, se necesita de un delincuente experto en el engaño o la manipulación. Se reduce el costo de un ataque exitoso (no es más necesaria la *expertise* técnica) y aumenta el beneficio (son las personas el objetivo y las que realizan las acciones y son ellas, generalmente, el eslabón más débil por no contar con la capacitación necesaria sobre los riesgos en el mundo digital). Esta técnica para la manipulación de personas es lo que se conoce como ***"Ingeniería social".*** En ella se emplean artilugios humanos y sociales para engañar a una persona y que sea esta persona quien ejecute una acción, brinde acceso al sistema o información a un delincuente que le permitan lograr su cometido. Un detalle importante para destacar es que la Ingeniería social, no tiene por qué ser una técnica únicamente utilizada para fines malignos o para la delincuencia. Por ejemplo, podría ser utilizada como forma de obtener información a un cliente cuando éste no sabe lo que quiere sobre un producto o necesidad. Un ejemplo burdo podría ser cuando un cliente va a una ferretería y necesita *"el cosito que va en el coso"*. Está en las habilidades de quien atiende intentar conocer qué es lo que quiere ese cliente y darle el objeto adecuado y esto lo consigue por su experticia en el campo y por las habilidades que tenga para poder "sacarle" información a un potencial cliente. La confianza es fundamental para aplicar la Ingeniería social, ya sea para fines malignos o benignos.

Volviendo al tema que es competencia del presente artículo, una de las formas más clásicas de la Ingeniería social es la **suplantación de identidad** o también conocida como *"phishing"*. En ella, los delincuentes, toman la forma de otra persona o institución para entablar un diálogo con el usuario o persona, lograr que esta confíe en ellos y así, obtener la información deseada. Una de las formas más comunes de phishing es el correo electrónico suplantando identidad, por ejemplo, de una tarjeta de crédito/débito o banco, donde se recibe un correo informando que la cuenta fue bloqueada y que se debe ingresar nuevamente al sitio (que será falso) para ingresar las claves de acceso al portal para validarse nuevamente. Al ingresar a un sitio falso, que parece ser igual que el real, la víctima ingresa las claves y automáticamente son robadas por los delincuentes. Imagínese si la persona que ingresa es la del área de contaduría o tesorería y les roban las claves de acceso de la cuenta bancaria de esa organización pública. Otra forma también puede ser algún correo que indique descargar un archivo, que está adjunto, para su visualización o que requiera ser completado. Este archivo podría ser un malware que, al descargarse y ser ejecutado por el propio usuario, podría infectar al dispositivo donde se descargó o bien, podría

diseminarse por toda la organización, infectando a un sinnúmero de dispositivos, dejando a la organización totalmente inoperativa.
Es por esto que el ataque a las personas es la principal causa de los diferentes incidentes o eventos adversos que reciben las organizaciones en general y por esta misma razón es que es necesario capacitar y concientizar a las personas sobre un uso seguro y responsable de los medios digitales. Capacitar para prevenir y concientizar para que se conozcan los riesgos al navegar y utilizar estos medios digitales. Pero esto no es todo, también es imperioso que las organizaciones cuenten con políticas en ciberseguridad, que se tomen decisiones que hagan un ecosistema seguro. La toma de decisiones, la generación de políticas al respecto, harán que las capacitaciones y concientizaciones sean efectivas dentro de una organización.

Conclusiones

En un mundo cada vez más digital donde tanto las organizaciones como las personas realizan cotidianamente diferentes actividades mediante el uso de la tecnología, es imperioso que se conozcan los riesgos que pueden estar presentes. Los delincuentes informáticos estarán siempre atentos a los descuidos, fallas en los sistemas o bien, al desconocimiento de las personas para intentar robar información o infectar los dispositivos que utilizan. Es por ello que se debe ser consciente de los riesgos, conocer las formas de ataque que utilizan estos delincuentes para afectar el patrimonio, intimidad, privacidad de las personas o las organizaciones.
En primer lugar, se debe poner a la ciberseguridad como prioridad en cualquier organización. Además, se debe ***"cambiar el verbo": no es gastar, es invertir.*** La inversión posibilitará una reducción de la probabilidad de que los eventos adversos o amenazas ocurran y también, posibilitará la reducción del impacto cuando estos eventos o amenazas suceden. Se debe tener siempre varias premisas a la hora de utilizar Internet o bien, exponer servicios allí. La primera de ellas es que ningún sistema es 100% seguro y la segunda, como consecuencia de la primera, es que será objeto de diferentes ataques. Un sistema no es 100% seguro porque constantemente se van descubriendo fallas que hacen que sea vulnerable y además, y es la causa principal, es desarrollado y operado por personas, siendo ellas, también vulnerables.
Para poder hacer frente a estas situaciones, es primordial que exista un plan político en materia de ciberseguridad. La toma de decisiones será fundamental para estar prevenido, para actuar y reaccionar frente a un evento adverso. Y esta toma de decisiones debe poner foco en la concientización y capacitación a los usuarios y personas ya que son el principal objeto de ataque de los delincuentes.

Bibliografía

- Sain, G. (2021); *Nuevas modalidades delictivas en materia de cibercrimen durante la pandemia del covid-19 en la república argentina;* En Revista Temas de Derecho Penal y Procesal Penal; Erreius Online.
- Kaspersky Lab; *¿Qué es un ataque de fuerza bruta?;* https://latam.kaspersky.com/resource-center/definitions/brute-force-attack.
- JEFATURA DE GABINETE DE MINISTROS. SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN (2019); *Resolución 1523/2019. Anexo II - Glosario de Términos de Ciberseguridad*.