EDITORIAL

Network security in communications: Perspectives and challenges

When discussing the concept of security associated with Information Technology (IT), it is not uncommon to find some confusion between information security and cybersecurity terminology. While the first focuses on protecting information and the assets that manage it, the second focuses on information in its digital form. Additionally, approaches from an information security perspective are commonly taken from a theoretical/normative standpoint, while cybersecurity-related techniques currently have both defensive and offensive approaches. This article addresses, in particular, the security of communications networks, which allow the interconnection between different end systems, involving not only communications equipment but also the physical media through which digital information is transported. Furthermore, the protection techniques used today are not restricted only to defensive mechanisms; thus, this editorial will not be limited to either the information security or cybersecurity perspective but a synergy of both. Regardless of the methods used in the IT area, the aim is to maintain confidentiality, availability, and integrity of data.

Main Causes of Network Security Problems

From a technical point of view, it is important to remember that the protocols used for communication in today's networks have their origins in the '70s. These protocols were not developed with a security perspective, inheriting a considerable technological deficiency. While it is true that many of these have been reworked over time, it is still possible to find infrastructures that have not incorporated all the improvements available to enhance communications infrastructure. Technological deficiencies are not exclusively the responsibility of the protocols; they are also present in the operating systems and applications that operate devices, which are not exempt from errors in their development and must be updated or patched as required. The technical knowledge of the person performing the configuration is another variable, as many manufacturers incorporate proprietary security features to make the platforms robust. Any failure to follow these best practice guidelines or recommendations could impact the weaknesses that a communications infrastructure may have. Furthermore, it is important to add to the accidental conditions, those deliberate actions that can put devices and communication media at risk, and those that do not result from human actions, such as environmental conditions.

Defensive Views of Network Security

Perhaps most organizations' traditional security mechanism consists mainly of tactics to protect, detect, and react to an attack that attempts to compromise the organization. Initially, this view, rather than being a structured process, was more instinctive and remained so in smaller organizations. In major infrastructures, it is a controlled process in which different defense schemes, such as the defense in depth model, an approach derived from military strategies where a series of barriers are defined to counterattacks with different obstacles, to make containment more effective. From the perspective of communications networks, some of the focuses of attention are the following:

IT Governance and Management: There must be an alignment between business objectives and information technologies; this implies the presence of a structured model that considers roles and responsibilities, internal capabilities, or outsourced services, and even the acquisition of equipment must be supported by a management model of governance of the organization. Technically speaking, there are different levels of documentation (policies, standards, and procedures). For the construction

of high-level documents, there is currently a wide range of information security frameworks that allow their development. Some sectors require special regulations, such as data protection or specific standards that regulate the type of information they store, process, or transmit. At the other extreme, procedures must be precise at the technical level to meet business requirements at higher levels.

Design and architecture: Network architecture traditionally focused on operation, but currently, this task is not only limited to hierarchical issues in the distribution of equipment; modular, resilient, and flexible designs must also comply with security recommendations, which in addition to availability, consider the confidentiality and integrity of the information being transported, incorporating zero trust models and the integration of new technologies.

Physical Security: This component relates to physical access to the infrastructure. From the point of view of communications networks, physical access is a critical issue to consider, given that the network, in its access layer, interacts directly with the users. Furthermore, connection to service providers means that the media used for data transport in the external plant may be exposed to human or environmental interventions.

Perimeter Security: This allows delimiting external and internal spaces of the organization; through communication devices, it is possible to outline areas and indicate which zones can communicate with each other, even specifying the direction of the origin of the traffic. Associated systems are intrusion detection or pprevention systems, traffic analysis platforms, network segmention, and Virtual Private Network (VPN).

Good network security practices: All protections that make it possible to configure communications devices should be incorporated here robustly. Practical security recommendation guides are available, such as those of the Center for Internet Security (CIS) and the recommendations provided by the manufacturers. Considering recommendations for the different communications devices is a complex undertaking, as protection will depend on variables such as network design, brands used, and the technical expertise of device administrators. It is important to ensure consistency between the organization's documentation on procedures, architecture, and business objectives for this process to work correctly.

Offensive Views of Network Security

Incorporating the defensive component in security strategies makes it possible to assess the risk, level of exposure, and capabilities of detection, prevention, and reaction to an incidence, in a scenario similar to that of an actual attack; with this data, it is possible to determine the impact of an attack on the business. Conducting these exercises should be part of a continuous process, allowing modifying the organization's strategy from reactive to proactive, directly benefiting the continuous improvement processes.

Several frameworks, such as Cyber Kill Chain or Mitre ATT&CK, guide the offensive process from the initial planning stage to documentation and reporting, dealing with digital attack vectors and physical and human components. Depending on the methodology, various phases are defined that are used in the attack process; in this document, they will be analyzed in two major stages:

Recognition and preparation: The reconnaissance phase intends to identify system weaknesses, which can be further subclassified from inside and outside the organization. External analysis can be performed without direct connection to the organization (for example, using traditional or specific search engines for analyzing devices connected to the Internet). It is common to find access to

administrate devices exposed to the Internet, and direct connections to the organization can be made by searching for remote device management mechanisms. In cases where the reconnaissance phase has access to the internal network, passive traffic analysis can be performed in search of weaknesses or active searches (which should be identified by the organization's defense team).

System exploitation: This device breach can be done through an unpatched vulnerability or defects in the device configuration. Attacks can be carried out by directly affecting the administration of the device (administration plane); in this case, the attacker can obtain total control of the device, which could directly affect the availability or degradation of the service. It is important to consider that many communications devices are starting points for VPN, potentially affecting the confidentiality of information. Additionally, communications devices allow network segmentation, which makes it possible to manipulate access to any independent segment, which would directly affect the organization's perimeter security. In cases where the disruption is directed at the data plane, it carries the information of the end systems, which can allow access to data that is not protected at the application level. Finally, the control plane is perhaps one of those that can pay the best returns for attackers since it is directly involved in communications protocols, allowing control of the device's switching functions, which can allow traffic redirection or spoofing of trusted sources or destinations. Communication protocols can also transport information outside the organization by exfiltrating data or generating communication channels for command and control systems to communicate outside the infrastructure.

New Challenges for Network Security

New technologies aim at virtualization, software-defined networks, cloud technologies, and the transport of larger volumes of information, presenting a major challenge to those who protect networks. Virtualization brings extra layers that require attention, as systems are not mounted directly on the hardware but on a software layer that can also have weaknesses. Regarding software-defined networks, centralized functions are incorporated, which, if affected, can compromise all network devices, besides the use of APIs (Application Programming Interface), which may also present weaknesses. Another important point to consider is cryptography, which can be affected by quantum computing; many of the current security mechanisms that exchange keys (asymmetric cryptography) can be compromised by these changes. Ultimately, traffic volumes and encryption functions make it increasingly complex to analyze malicious traffic patterns. Consequently, new techniques must be used to complement the "new generation" functions in networks, some of which are no longer current and require sophisticated mechanisms for protection, including ML-based analysis systems.

Mag. Daniel Sebastián Pacheco
Lesand Community Founder
Santiago, Chile
dpacheco@lesand.org

EDITORIAL

Seguridad en redes de comunicaciones: Perspectivas y desafíos

Cuando se habla del concepto de seguridad asociado a las Tecnologias de la Informacion (TI), es común encontrar confusión entre conceptos como seguridad de la información y ciberseguridad. El primero posee un enfoque en la protección de la información y los activos que la gestionan, mientras que el segundo, se centra en la información en su forma digital. Además, los enfoques desde la perspectiva de la seguridad de la información comúnmente se realizan desde una mirada teórica/normativa, mientras que en la actualidad las técnicas relacionadas con ciberseguridad poseen enfoques defensivos y ofensivos. Este artículo trata en particular, sobre la seguridad en redes de comunicaciones las cuales permiten la interconexión entre diferentes sistemas finales, lo que involucra no solo a equipos de comunicaciones, sino que también a los medios físicos por donde se transporta la información digital. Por otro lado, las técnicas de protección usadas en la actualidad no se restringen solo a mecanismos defensivos, por lo cual esta editorial no se limitará únicamente a una perspectiva de seguridad de la información o ciberseguridad, sino a una sinergia de ambas. Independiente de los métodos en el área de las TI se busca mantener la confidencialidad, disponibilidad e integridad de los datos.

Principales causas de los problemas de seguridad en redes

Desde una mirada técnica es importante tener en cuenta que los protocolos utilizados para la comunicación en las redes actuales tienen sus orígenes en la década de los 70, estos protocolos no fueron diseñados con una perspectiva de seguridad, lo que hereda una deficiencia tecnológica considerable. Si bien es cierto, muchas de estas se han enmendado con el tiempo, aún es posible encontrar infraestructuras que no han incorporado todas las mejoras disponibles para robustecer la infraestructura de comunicaciones. La deficiencia tecnológica no es exclusivamente responsabilidad de los protocolos, también está presente en los sistemas operativos y aplicaciones que controlan los dispositivos, los que no se encuentran exentos de errores en su desarrollo y deben ser actualizados o parchados según corresponda. Otra variable por considerar corresponde al conocimiento técnico de quien realiza la configuración, ya que muchos fabricantes incorporan diferentes características de seguridad propietarias que permiten robustecer las plataformas. El no seguir estas pautas de buenas prácticas o recomendaciones, también influyen en las debilidades que pueda tener una infraestructura de comunicaciones. Adicionalmente a las condiciones accidentales, hay que agregar aquellas acciones deliberadas que pueden poner en riesgo los dispositivos y los medios de comunicación, así como también aquellas condiciones que no dependen de las acciones humanas, como las condiciones ambientales.

Visión defensiva de la seguridad en redes

Esta visión de la seguridad es quizás el mecanismo más tradicional para encontrar en la mayoría de las organizaciones, la cual consiste principalmente en tácticas que permitan proteger, detectar y reaccionar a un ataque que intente comprometer a organización. Inicialmente esta visión, era un proceso más instintivo que estructurado el cual se sigue manteniendo así en organizaciones pequeñas. En infraestructuras de mayor tamaño, es un proceso estructurado, en el cual se utilizan diferentes esquemas de defensa, como por ejemplo el modelo de defensa en profundidad, un planteamiento que proviene de las estrategias militares donde se definen una serie de barreras que pretenden debilitar los ataques con diferentes obstáculos, de forma tal que la contención sea más efectiva. Desde la perspectiva de las redes de comunicaciones algunos de los focos donde poner atención son los siguientes:

Gobernanza y Gestión TI: Debe existir una alineación entre los objetivos del negocio y las tecnologías de información, esto implica la articulación de un modelo estructurado que considere roles y responsabilidades, capacidades internas o servicios tercerizados e incluso la adquisición de equipamiento debe sustentarse en un modelo de gestión de gobierno de la organización. Desde una mirada técnica existen diferentes niveles de documentación (políticas, normas y procedimientos). Para la construcción de documentos de alto nivel existen en la actualidad una amplia gama de marcos de trabajo de seguridad de la información que permiten la construcción de estas. Además, ciertos sectores requieren regulaciones especiales como por ejemplo normativas relacionadas con la protección de datos o estándares específicos que regulan el tipo de información que almacenan, procesan o transmiten. En el otro extremo, los procedimientos deben ser muy específicos a nivel técnico para que puedan cubrir los requerimientos del negocio planteados en niveles altos.

Diseño y arquitectura: Tradicionalmente el foco de la arquitectura de red se enfocaba en la operación, actualmente esta tarea no se limita solo a temas jerárquicos en la distribución del equipamiento, diseños modulares, resilientes y flexibles. También deben cumplir recomendaciones de seguridad, en los cuales además de importar la disponibilidad, se debe considerar la confidencialidad y la integridad de la información que se transporta, incorporando modelos de confianza cero y la integración de nuevas tecnologías.

Seguridad Física: Esta componente se relaciona con el acceso físico a la infraestructura, desde el punto de vista de las redes de comunicaciones es un tema crítico por considerar, ya que la red, en su capa de acceso, interactúa directamente con los usuarios. Además, desde el punto de vista de la conexión a los proveedores de servicios, los medios usados para el transporte de datos en la planta externa pueden estar expuestos a intervenciones humanas o ambientales.

Seguridad Perimetral: Permite delimitar espacios externos e internos de la organización, a través de dispositivos de comunicaciones es posible definir áreas e indicar que zonas se pueden comunicar entre sí, incluso indicando la dirección del origen del tráfico. Asociados a esta se encuentran sistemas de detección o prevención de intrusiones, plataformas de análisis de tráfico, segmentación de redes y Virtual Private Network.

Buenas prácticas de seguridad de red: Acá se deben incorporar todas aquellas protecciones que permitan robustecer las configuraciones de los dispositivos de comunicaciones. Existen guías con recomendaciones prácticas de seguridad como las del *Center for Internet Security* (CIS) y las recomendaciones que entregan los mismos fabricantes. Considerar recomendaciones en los diferentes dispositivos de comunicaciones es una tarea compleja, ya que la protección dependerá de variables como el diseño de la red, las marcas utilizadas y la capacidad técnica de quienes administran los dispositivos. Es importante para que este proceso funcione correctamente que exista una coherencia entre la documentación de la organización en sus procedimientos, la arquitectura y los objetivos del negocio.

Visión ofensiva de la seguridad en redes

La incorporación de la componente ofensiva en las estrategias de seguridad permite evaluar el riesgo, el nivel de exposición y las capacidades de detección, prevención y reacción ante un incidente, en un escenario similar al de un ataque real, con estos antecedentes es posible demostrar el impacto de un ataque en el negocio. La realización de estos ejercicios debe ser parte de un proceso continuo, lo que permite modificar la estrategia de la organización de reactiva a proactiva, lo que beneficia directamente a los procesos de mejora continua.

Existe una serie de marcos de trabajo, como por ejemplo Cyber Kill Chain o Mitre ATT&CK que permiten guiar el proceso ofensivo desde la etapa inicial de planificación hasta la documentación y generación de informes, las cuales no solo se preocupan de los vectores de ataque digitales, también incluyen componentes físicas y humanas. Dependiendo de la metodología se definen una serie de fases que se utilizan en el proceso de ataque, en este documento se analizarán en dos grandes etapas:

Reconocimiento y preparación: La instancia de reconocimiento busca identificar debilidades del sistema, las cuales se pueden subclasificar a su vez desde el interior de la organización o desde el exterior de esta. Aquellos análisis desde el exterior se pueden realizar sin conexión directa a la organización (por ejemplo, uso de buscadores tradicionales o específicos para el análisis de dispositivos conectados a internet) es común encontrar acceso a la administración de dispositivos expuestos a internet. También se pueden realizar conexiones directas a la organización en búsqueda de mecanismos de administración remota de los dispositivos. En aquellos casos que quien realiza la fase de reconocimiento tiene acceso a la red interna desde acá se pueden realizar análisis pasivos del tráfico en busca de debilidades o búsquedas activas (las cuales debieran ser identificadas por quien realiza la defensa de la organización).
Explotación del sistema: Este compromiso de los dispositivos puede realizarse a través de alguna vulnerabilidad no parchada o por defectos en la configuración del dispositivo. La explotación se puede realizar afectando directamente la administración del dispositivo (plano de administración), en este caso el atacante puede obtener control total del dispositivo, esto puede afectar directamente la disponibilidad o la degradación del servicio, por otro lado es importante considerar que muchos de los dispositivos de comunicaciones son puntos de inicio de redes VPN, lo que puede afectar a la confidencialidad de la información; adicionalmente los dispositivos de comunicaciones permiten la segmentación de redes lo que permite manipular el acceso a cualquier segmento independiente, lo que afectaría directamente a la seguridad perimetral de la organización. En los casos de que la afectación se dirige al plano de datos, este transporta la información de los sistemas finales, el cual puede permitir el acceso a los datos que no estén protegidos a nivel de aplicación. Finalmente, el plano de control es quizás uno de los que puede entregar mejores dividendos a quienes realizan pruebas ofensivas, ya que en este encontramos directamente protocolos de comunicaciones, los que permiten controlar funciones de conmutación del dispositivo, lo que puede permitir la redirección del tráfico o la suplantación de orígenes o destinos de confianza. Adicionalmente, los protocolos de comunicaciones también pueden ser usados para transportar información fuera de la organización realizando exfiltración de datos o generando canales de comunicación para que se comuniquen sistemas de comando y control desde el exterior de la infraestructura.

Nuevos desafíos para la seguridad en redes

Las nuevas tecnologías apuntan a la virtualización, redes definidas por software, tecnologías Cloud y el transporte de volúmenes de información mayores, lo que presenta un gran desafío a quienes protegen las redes. La virtualización agrega más capas en las cuales se debe poner atención ya que los sistemas no se montan directamente en un hardware, si no que sobre una capa de software que también puede tener debilidades. En relación con las redes definidas por software se incorporan funciones centralizadas las cuales en caso de ser afectadas estas pueden afectar a todos los dispositivos de red, además del uso de APIs (del inglés *Application Programing Interface*) las cuales pueden presentar debilidades también. Otro punto importante a considerar es la criptografía, que se puede ver afectada por la computación cuántica, muchos de los mecanismos de seguridad actuales que intercambian llaves (criptografía asimétrica) se pueden ver comprometidos con estos cambios. Finalmente, los volúmenes de tráfico y las funciones de cifrado hacen que cada vez sea más complejo analizar patrones de tráfico malicioso, lo que implica el uso de nuevas técnicas que complementen las funciones de "nueva generación" en las redes, las cuales ya no son tan nuevas y requieren mecanismos más sofisticados para la protección como sistemas de análisis basados en Machine Learning (ML), por ejemplo.

Mag. Daniel Sebastián Pacheco
Fundador Comunidad Lesand
Santiago, Chile
dpacheco@lesand.org