infraestructura tecnológica con soporte a la Internet o los servicios con la Nube.

Así por ejemplo, el Departamento de Defensa de los EEUU (DoD) percibe al ciberespacio como un Dominio Global y en 2011 declaró, lo siguiente como parte de su estrategia de defensa del Ciberespacio: "*El DoD usa el ciberespacio para habilitar sus operaciones militares, de inteligencia y negocios, incluyendo los movimientos de personal y materiales, así como el comando y control del espectro completo de sus operaciones militares*".

Por otra parte, en las últimas décadas, los incidentes directos e indirectos en todo el mundo, sobre plantas nucleares, industriales, eléctricas, aeropuertos y hospitales, han crecido. Algunos se han derivado de fallas básicas como es la actualización de una protección del tipo antivirus, incrustado en un Sistema Operativo [4]. Mientras que otras fueron dirigidas y específicas a un blanco, como es el caso de Stuxnet y los sistemas con tecnología centrífuga de la planta de desarrollo nuclear de Irán [5].

En 2020 los investigadores Sungjoong, Jiwon, Haengrok, Dongil y Dongkyoo sostuvieron en un trabajo de IEEE Access que: "*La ciberguerra ocurre en el ciberespacio y está siendo procesada y generada a través de varios ciber ataques, tales como el hackeo de sistemas de información militar de otros países y paralizando sistemas militares y de información para la defensa que permiten alcanzar objetivos militares*" [6]. Este panorama delicado, no son los "hacking" de finales de los noventa, sino que también incorpora naciones – estados atacando y defendiendo su ciberespacio y vínculo con su soporte al espacio real, lo cual obliga a que los profesionales de computación se replanteen preguntas básicas.

Dudas sobre la inseguridad que verdaderamente rodea los desarrollos y artefactos tecnológicos de soporte crítico, para servicios básicos, sistemas de producción y economía moderna. Consultas como: ¿el esquema para desarrollar un sistema y luego colocar controles y protecciones, es suficientemente bueno y sólido para las necesidades?. Adicionalmente, si se diseñan sistemas teniendo presente las necesidades y requerimientos de seguridad desde su inicio, ¿verdaderamente se puede anticipar todos los peligros y cambios de contexto que un mundo exterior puede producir?.

Basta con mirar la variedad y sofisticación de los ataques informáticos de nuestros días, así como las cifras de pérdidas económicas por fallas de ciberseguridad, para vislumbrar la respuesta del caso. Finalmente, también hay espacio para la cuestión central de esta reflexión: ¿el resguardo de un sistema crítico debe apoyarse en el mismo tipo de instrumentos y técnicas de seguridad, que se incorporan en un sistema informático común, o amerita un modo diferente y más profundo de concepción?

3. Tecnología Crítica con Base al Pensamiento de Fitch y Muckin

Tomando la idea central de las arquitecturas que se defienden, se puede enumerar los siguientes aspectos que deben guiar el trabajo de diseño de los sistemas críticos:

- Los sistemas no siempre operan en las mismas condiciones, su contexto cambia y ello potencialmente incide sobre la inseguridad de fuente externa. En consecuencia, sus respuestas funcionales no siempre deben ser las mismas.
- La exposición y visibilidad del sistema ante el mundo exterior, debe poder ser reducida si así se requiere.
- La concepción de un sistema crítico se debe soportar en la aplicación de una inteligencia adaptativa, que pueda responder ante la presencia y comportamiento de cualquier ataque.
- Las protecciones deben responder a las técnicas de los atacantes, al igual que a las nuevas amenazas. Por ser sistemas de naturaleza crítica, la guía X.800 ITU-T de los servicios de seguridad no es el elemento determinante. Es un complemento para enfocar.
- El diseño interno debe ofrecer variaciones en su funcionalidad, haciendo progresiva la fortaleza de su defensa. De ser necesario, debe presentar, selectivamente, una representación falsa del sistema.
- La inter-relación humana es indispensable y comprende las acciones agresivas. Como los ataques se responden en menos que segundos, las máquinas son ideales para eso, pero detectar si lo que ocurre es un falso positivo, una distracción o es la esencia de un verdadero mal, es algo que los humanos entrenados aún hacen mejor. La decisión de atacar debe privilegiar lo humano.
- En semejanza con los seres humanos, ante un peligro inminente, la última defensa es "correr o pelear". Por ello el sistema crítico deberá considerar la disyuntiva, no excluyente, entre migrar datos, operaciones y/o agredir.

Por otra parte, existen aspectos que son ejes de soporte en la seguridad final del diseño y deberán ser atendidas con métodos no necesariamente clásicos. El primero de ellos se vincula con las relaciones y dependencias basadas en la confianza del sistema.

4. El Diseño de Sistemas Críticos y la Confianza

Un elemento relevante en el diseño de los sistemas críticos es la confianza y ello incide en momentos de peligro. Los sistemas tradicionales se elaboran teniendo en mente una confianza estática. Este es el caso de una actualización de software del fabricante que se dispara automáticamente, el de una cuenta de usuario privilegiada que todo lo puede hacer, o tal vez el de una autenticación única de usuario o aplicación ("Single Sign-On"), que provee acceso a todo un ambiente de red. Otro caso es el de un rango de direcciones de redes predefinidas y reconocidas como válidas, o segmentos de tráfico en las comunicaciones que de acuerdo al perímetro lógico se dan como "confiables" o incluso, pudiera ser el de conexiones de servicio y/o mantenimiento "amigables", que fabricantes y/o proveedores actualmente incluyen en sus contratos. El problema es que si uno de esos elementos se compromete, tradicionalmente, las protecciones no lo reconocen y no pueden responder apropiadamente. Se sigue considerando que son fiables y pueden ser mal aprovechadas.

De forma que esa aproximación tan comúnmente usada, puede ser contraproducente para un sistema crítico, ya que a menudo los atacantes explotan las debilidades de confianza y con ello penetran o extienden su ámbito de acción. Luego, es posible suponer que la confianza debe variar y en situaciones de riesgo o ataque, reducirse sustancialmente para facilitar una mejor protección. La noción fundamental es que la confianza sostenga la ejecución de las operaciones e intercambios y de ser requerido, pueda alterar la funcionalidad "normal" del sistema crítico.

La Figura 1 representa, sobre un sistema crítico, un esquema simple para manejar diferentes consideraciones dinámicas de la confianza.

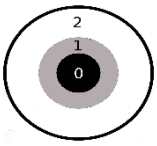

Figura 1: Esquema Jerárquico de la Confianza

A través de tres círculos concéntricos, que representan la extensión de la confianza, se puede apreciar cuál conjunto contiene a otro. Así pues, de adentro para afuera está el nivel "0" de confianza, que es mínimo y se visualiza como el núcleo. Ese ámbito refleja las Relaciones de Confianza Básicas y comúnmente refiere la de administradores y operadores locales, así como aplicaciones propias, no en red. Se espera también, que este nivel predomine en situaciones de ataques, donde hay que disminuir las suposiciones y creencias. El nivel "1", que se ve como intermedio, amplia la confianza a un área de Relaciones de Confianza Regionales, es decir, donde se puede aceptar que las redes locales y/o dominios corporativos son "amigables". El ámbito externo queda afuera de este nivel, por lo cuál ha sido concebido para ejecuciones de riesgo moderado o de sospecha. El último nivel, identificado por "2", que se ve como el círculo más externo, incluye objetos y asociaciones de confianza con el exterior del sistema. En situaciones de tranquilidad pudiera llegar a fronteras con los proveedores conocidos de suministros, servicios y/o comunicaciones, que interconectan con la Red de Redes.

Colateralmente, la decisión de cuál nivel de confianza debe ser el vigente puede permitirse que sea automatizada, bajo supervisión de indicadores, métricas y perfiles históricos, siendo lo común que se escale gradualmente, pero debe aceptarse la intervención explícita y humana para fijarla arbitrariamente. Una manipulación, que por ninguna razón debe ser remota y bien puede exigir doble autorización de entes diferentes, en ubicaciones separadas y con factor de autenticación triple.

5. El Estado y el Diseño de Sistemas Críticos

Otro elemento de importancia que resulta ser una columna sobre la que se edifica la seguridad de un sistema crítico, es su condición operacional. A eso y a la inteligencia recabada de señales de riesgos de su contexto, denominamos estado. El estado define la "salud y situación" del sistema crítico y en consecuencia, su capacidad funcional y la atención ante el exterior. Un sistema bajo ataque deberá tener un estado que como tal lo represente y activar o reforzar sus medidas de salvaguarda o respuesta, ante tal condición.

Un modelo simple de estado incluye cuatro categorías: normal, atípico, en-riesgo y bajo-ataque.

- Normal: El sistema opera con sus *relaciones de confianza* pre-establecidas y sus medidas de protección tradicionales. En principio, se puede esperar que este estado se corresponda con un nivel de confianza "2".
- A-típico: emite alertas y eleva los niveles de supervisión. Hay observación y comparación de las relaciones de confianza contra su perfil tradicional. Se refuerza el uso de indicadores y métricas estadísticas. Bien puede acoplarse con los niveles "1" y "2". También emplea técnicas de Inteligencia Artificial para gestionar los riesgos presentes.
- En-riesgo: eleva considerablemente los niveles de protección, control y supervisión; internamente registra todo la actividad que puede y no atiende nuevas peticiones, que no sean las tradicionales. Emite alertas sobre todos los niveles y rechaza relaciones de confianza indirectas. Opera con la salvaguarda de "bajo extrema emergencia" se estacionará en un "área de resguardo temporal". Se asocia con los niveles de confianza "0" o "1".
- Bajo-ataque: No atiende nuevas peticiones, hay selectividad en lo que ya se realiza y se limita el flujo de información. Se elevan los controles y protecciones a su máxima capacidad. Se bloquean servicios no críticos y se inicia procedimientos internos de contingencia (incremento de alertas, comunicación de su condición a sistemas con los que se colabora, transferencia de funcionalidades, activación del respaldo y se puede activar la migración de datos sensibles). Si no hay respuesta estratégica, sigue tácticas disuasivas o de confusión hacia el exterior. Es fundamental que se registre todo lo que se pueda afuera de sí mismo y si no se obtiene apoyo, progresivamente el sistema se desactiva. Se reduce la confianza a su nivel núcleo, "0".

Al contrario de lo que a menudo los diseñadores presumen, hay que considerar situaciones de final no feliz. Posibilidad de que el sistema no posea las defensas adecuadas para manejar algún ataque. A eso lo llamamos "situaciones extremas".

6. Situaciones Extremas y las Directivas Humanas

Una diferencia notable entre un sistema informático y un sistema crítico, deberá ser su ajuste en la estrategia de defensa que se aplique. Desde un nivel estrictamente defensivo a otro que incluya acciones ofensivas; algo propio de ciberconflictos y/o ciberguerras. Obviamente, este giro debe contar con la autorización humana y nuevamente, puede ser necesario que esta sea dual e incorpore tecnologías biométricas.

La Figura 2 describe una organización lógica de una potencial arquitectura, reflejando los perímetros de defensas y el externo al sistema. También presenta un espacio de instrumentos para soportar pasivamente o para hacerlo, con acciones agresivas.

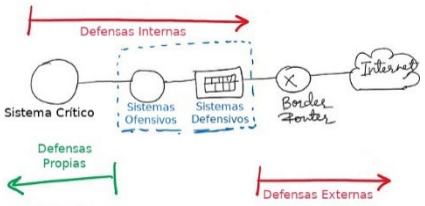

Figura 2: Arquitectura con Defensas y Armas

Esa gráfica expone áreas que rodean al sistema crítico e ilustra zonas para defender. Hay defensas externas que inician en el enlace con los proveedores de comunicaciones y servicios con la Internet (ISP). Otras defensas son internas y graduales, llegando hasta ser propias y particulares del mismo sistema crítico. Entre ambas áreas existen entidades para protecciones defensivas y otras hostiles. Estas últimas se emplean en situaciones de "supervivencia" del sistema crítico y aplican en caso de ataques, que saturan o sobrecargan, como las del tipo Negación de Servicio Distribuido (DDoS).

Estos escenarios pueden ser el último recurso para evitar apagar al sistema como protección final. Llegar a una desactivación tan drástica, es la última defensa y únicamente tiene por objetivo preservar al sistema para otra ocasión, pero su razón de ser podría haberse perdido. Entonces resulta lógico esperar que este tipo de situaciones no sean propias de ambientes tradicionales y se acomodan, a otras más cercanas a la guerra. Las valoraciones y decisiones a seguir en esos conflictos escapan de la construcción técnica, pero deben poder ser instrumentadas con apoyo tecnológico.

7. Controles, Procedimientos y Principios de Seguridad

Para completar la etapa de diseño se debe poder estipular los procedimientos que permitirán tratar con la capacidad de inteligencia de la seguridad del sistema. Para ello continuamente habrá que adaptar el Modelo de Amenazas, lo cual constituirá un proceso propio del sistema crítico, relacionado con su propia seguridad. En otras palabras, esto se constituye como un mecanismo de cuidado del mismo y sobrepasa la simple activación de un control o una protección. Un procedimiento que incorpora un nivel de inteligencia para cambiar de forma según se demanda, a modo de morfogénesis.

Resulta necesario agregar que los procesos y procedimientos de seguridad, deberán estar alineados con aquellos principios de seguridad de Saltzer y Schroeder [7] que sean escogidos. Entonces, en función de los resultados se pueden establecer los controles, las protecciones, los modelos y las técnicas que soportarán todos esos mecanismos. Cada uno de estos son diferentes pero se relacionan, armoniosamente, entre sí. Por ejemplo, un modelo para establecer la aleatoriedad de una "función hash" o de un mecanismo criptográfico, puede ser el modelo de seguridad del oráculo [8]. Mientras que la herramienta que instrumenta la función matemática señalada, es un instrumento que puede ser empleado por un procedimiento, para determinar si dos secuencias de bits son iguales. Con ello se puede tener la facultad de determinar si un archivo, por ejemplo, fue alterado en su contenido o si se corresponde con lo que antes se transmitió en forma protegida.

Por otro lado, una técnica de seguridad es por ejemplo el uso de señuelos o distracciones. Este tipo de elementos pueden ser usados para construir medidas evasivas o ganar tiempo y se deben acomodar, dentro de procedimientos de defensa. Cuando y cómo habilitarlos dependerá de la inteligencia recabada y la evaluación de riesgos, que previamente se haya realizado. Algo que puede ejecutarse en tiempo real y así variar, según el peligro presente. Bajo esta aproximación, es posible deducir que el diseño que se realice puede obtener libertad o mucha flexibilidad, para los detalles de la futura implementación del mismo sistema. Aún cuando, hay una línea directriz suprema que regula y dirige la protección del sistema.

8. Colofón

Este trabajo ha descrito una serie de pautas lógicas que pueden guiar el diseño de seguridad de un sistema crítico, que además se apoya en la propuesta de Fitch y Muckin para sistemas con capacidad inteligente de defensa. Esto aspira a ser una alternativa al tradicional esquema de diseño de sistemas y luego colocar las protecciones, según se identifiquen los servicios de seguridad X.800 del ITU-T.

Referencias

[1] S. Fitch y M. Muckin, *Defendable Architectures Achieving Cyber Security by Designing for Intelligence Driven Defense*, LM White Paper, PDF, 2019. https://surl.li/hsjrbq

[2] N. Petru-Cristian. *Cyber Conflict and International Relations: A Comprehensive Analysis of Cyber Deterrence Strategies en Contemporary Geopolitics*. 10.13140/RG.2.2.29742.69449, 2024

[3] T. Berson y D. Dorothy. *Cyberwarfare*. IEEE Security & Privacy. 9. 13-15. 10.1109/MSP.2011.132, 2011.

[4] HKCERT, *CrowdStrike Denial of Service Alert*, HTML, Julio 2024. https://shorturl.at/2Vvka

[5] R. Langner, *To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve*, PDF, Noviembre 2013. https://shorturl.at/TVKIe

[6] S. Kim, J. Kang, H. Oh, D. Shin y D. Shin, *Operation Framework Including Cyber Warfare Execution Process and Operational Concepts*, IEEE Access, vol. 8, pp. 109168-109176, doi: 10.1109/ACCESS.2020.3001286. 2020

[7] J. Saltzer y M. Schroeder. *The Protection of Information in Computer Systems*, HTML.1975. http://www.cs.virginia.edu/~evans/cs551/saltzer/

[8] M. Bellare y P. Rogaway. *Random Oracles are Practical: A Paradigm for Designing Effecient Protocols.* Proceedings of the First ACM Conference on Computer and Communications Security, 1993.