EL CONTROL DE LA CONEXIÓN DE RECURSOS A UNA RED CORPORATIVA

Voy a compartir con ustedes un tema que creo de interés y que es de preocupar, o mejor, de mucho preocupar: **"El control de la conexión de recursos a una red corporativa"**. Y lo voy a abordar desde un punto de vista eminentemente práctico y de la realidad diaria, sabiendo que es una materia a la que los responsables de seguridad continuamente tenemos que hacer frente con contundencia y al mismo tiempo con unas grandes dosis de diplomacia.

Pretendo alejarme de los grandes conceptos y planteamientos, que a estas alturas del partido son plenamente conocidos y han sido sabiamente desarrollados en esta sección por otros colegas. Me estoy refiriendo a todo lo que sustenta metodológicamente la implantación de un SGSI y su continuo *feedback* atendiendo al modelo PDCA (Plan, Do, Check y Act), a las recomendaciones de la Norma UNE-ISO/IEC 17799 y a la Norma UNE 71502, que chequea la lista de controles de la 17799.

Control

Es en este escenario en donde se presenta uno de los grandes retos de la seguridad TIC: cómo controlar el acceso (la conexión de recursos) a una red corporativa que es, con respecto a la corporación, lo que una red de autopistas es con respecto a la economía de una nación, o la red neuronal con respecto al organismo humano. En todos los casos, el buen funcionamiento de dicha pieza clave es fundamental para que el resto de "recursos", "destinos" o "sistemas" reciba la "información", "mercancía" o "productos" que le son indispensables para realizar su propia actividad.

Nunca antes las compañías habían tenido que encarar tantos retos y en tantas direcciones. Y las "maravillas" que se pueden hacer con una red corporativa que posibilite el acceso a todos los recursos y servicios demandados: correo, Internet, accesos remotos, *wireless*, almacenamiento, intranet y sistemas de información corporativos, entornos y recursos de desarrollo, etc, hacen de ella un elemento crucial que hay que cuidar con especial mimo, ya que cualquier eventualidad significa que el resto de recursos (elementos) quedan "inutilizados", o mejor sería utilizar la palabra "inalcanzables".

En esta disciplina de la seguridad es conveniente –aún diría más, indispensable– tener aliados en la organización. Y éstos se ganan informando, argumentando, demostrando y convenciendo.

Antes de continuar, quiero participarles que el sustrato de todos mis comentarios tiene su etiología en la experiencia del desempeño de mi labor profesional en una gran corporación, en la que el negocio es en cada momento las necesidades del cliente. Resumiendo y en esencia, no lo que yo le ofrezco y Ud. me puede adquirir, sino lo que Ud. me solicita en cada momento y yo le voy a proporcionar.

Nos situamos entonces en corporaciones multinacionales, multiservicio, multiproducto, multimercado, en donde el "*core*" del negocio está íntimamente ligado con la información y el conocimiento, en áreas como las tecnologías de información, los equipos electrónicos de defensa o la simulación y sistemas automáticos de mantenimiento. O dicho llanamente, y dentro del ámbito en el que me quiero posicionar, donde la mayoría de los usuarios que acceden a los sistemas y servicios, tienen un nivel de conocimiento tecnológico realmente importante, por no decir que en algunas ocasiones impresionante.

Es entonces cuando queda plenamente justificado realizar una gestión y control exhaustivos, no sólo de quién se conecta a la red y con qué expectativas, sino también de qué recursos en cada momento están conectados o se quieren conectar a ella y en qué condiciones. Sabiendo de antemano, y aquí volvemos a incorporar uno de los condicionantes expuestos anteriormente, que al estar posicionados en una corporación multiservicio, multiproducto y multimercado, las necesidades de los diferentes proyectos y áreas a la hora de desplegar entornos de desarrollo, pruebas y nuevas tecnologías demandadas por los clientes, van a originar la proliferación de nuevas redes de proyectos y nuevos recursos conectados a la red corporativa con el único y crucial objetivo de dar servicio al cliente, obtener una cuota de mercado y cumplir las expectativas presupuestarias, pero no siempre teniendo en cuenta las normas existentes para salvaguardar la red de cualquier compromiso o incidente.

Llegados a este punto en el que tenemos encuadrado y planteado el foco de preocupación, hagamos un paréntesis para enfatizar que el tratamiento de este compromiso es de capital importancia en una gran corporación, que tiene muchas connotaciones, y que está latente de continuo, incluso después de haber lanzado y puesto en marcha desde una unidad encargada de velar por la seguridad de la entidad todos los mecanismos que requiere el actual concepto de seguridad gestionada.

Damos por supuesto que en este tipo de organizaciones se ha realizado una andadura importante a la hora de enfocar y gestionar la seguridad de acuerdo a los requisitos de Seguridad a conseguir, teniendo como referente los 10 dominios, 36 objetivos y 127 controles de la Norma UNE-ISO/IEC 17799:

- Requisitos de seguridad objetivo.
- Organización de seguridad.
- Política de seguridad corporativa.
- Difusión de normas y procedimientos.
- Diagnóstico de seguridad.
- Plan de seguridad.

Es decir, que se está inmerso en un proceso de implantación de la gestión de la seguridad sustentado en la tecnología, la política y normativa, y la auditoría.

La prevención

Pero vayamos a la realidad. Ya no estamos hablando de estrategias y políticas, sino del requerimiento diario, de la conexión física de cualquier recurso, ya sea servidor, estación de trabajo, puntos de acceso o cualquier otro elemento a la red corporativa, y la responsabilidad del Área de Seguridad si ello se hace descontroladamente y sin su visto bueno.

Si continuamos ahondando, y bajo la premisa de la gestión de la seguridad, disponemos, tanto técnica como normativamente, de los mecanismos y medidas necesarias (administración y monitorización de cortafuegos perimetrales y de internet, de *switches* y *routers*, gestión de antivirus y de alertas de seguridad, políticas y procedimientos, etc.) que permiten solventar de una manera rápida y eficaz cualquier incidente que comprometa la

red y relacionarlo, si es el caso, con el recurso que lo está ocasionando, evidentemente por no cumplir con la normativa aplicable, ¿somos, entonces, capaces de detectar el problema? Por supuesto. ¿Lo podemos solucionar? De inmediato. Pero debemos ser mucho mas ambiciosos, debemos pensar en medidas preventivas y no sólo paliativas.

Es entonces el momento de apostar por resolver el tema que nos preocupa y, teniendo presentes las soluciones de última generación, plantearse la implantación de tecnología que incorpore la gestión de las normas de seguridad de conexión de recursos a la red. Es decir pensar en identificar, auditar, evaluar y decidir si los candidatos o a veces polizontes deben o no pertenecer al "club". Ahora bien, no nos vamos a engañar, debemos analizar muy bien, y sobre todo en corporaciones de las características antes mencionadas, lo siguiente:

- En qué despliegue nos vamos a embarcar. Esfuerzo y coste.
- Las necesidades de administración de cada solución.
- Y, por supuesto, las repercusiones que estas medidas puedan tener en la organización, cuando al pasar a ser preventivas, en un momento determinado entren en conflicto las responsabilidades del área de Seguridad, que es garante de la seguridad del servicio, y las del área Operativa, que utiliza el servicio para generar negocio, objetivos ambos estratégicos.

El límite de la flexibilidad

Con toda la normativa a nuestro favor, y también sabiendo que es muy poco probable encontrar un mediador, ¿cómo ponemos la pica en Flandes sin que nadie de cierta relevancia pida explicaciones, o se oigan voces con argumentos como "el cliente lo requiere", "estoy generando negocio", "tenemos que ser flexibles" y algunos otros que seguro a todos se nos vienen a la cabeza?

Estamos, finalmente, abordando la verdadera dimensión y dificultad del tema. ¿Qué hacemos? ¿Primamos la seguridad como elemento común y vital a toda la corporación, o el servicio ágil y dinámico que también se nos exige y que tan necesario es para el negocio?

Como ven, he querido plasmar las dos alternativas extremas entre las cuales hipotéticamente "los chicos de seguridad" deberían elegir. Pero ese no es el camino. En esta disciplina de la seguridad, siempre es conveniente, aún diría más, es indispensable, tener aliados. Y estos se ganan informando, argumentando, demostrando y convenciendo. Pero tampoco nos debemos engañar, en muchas ocasiones vamos a tener que tomar arte y parte, y llegados a ese momento y siempre después de analizar cada caso con detenimiento, hemos de cumplir con nuestra responsabilidad con elegancia, pero, por favor, siempre con contundencia.

Las "maravillas" que se pueden hacer con una red corporativa que posibilite el acceso a todos los recursos y servicios demandados hacen de ella un elemento crucial que hay que cuidar con especial mimo, ya que cualquier eventualidad significa que el resto de recursos (elementos) quedan "inutilizados", o mejor sería utilizar la palabra "inalcanzables".

¿Cómo hacer?

En todas las disciplinas, decidir no es fácil, y menos en esta que nos compete, en la que en un porcentaje elevado de veces, no tomar ninguna decisión puede no conllevar graves consecuencias, pero que en otro porcentaje, aunque pequeño, puede originar un desastre a la organización en cuanto al compromiso de la disponibilidad, confidencialidad e integridad de la información. Se corre el riesgo de bajar la guardia. Se me viene a la mente una frase que utilizan mucho los profesionales de cierta disciplina en medicina, "90% de rutina y 10% de la acción más estresante que uno pueda imaginar".

¿Cómo soslayamos entonces esta aparente contraposición de objetivos?, y digo aparente porque todos tenemos claro que la meta final es la calidad y el buen hacer, y ahí están incluidos ambos. Pues de forma similar a como se hace en otras disciplinas del mundo de la tecnología:

Ante cualquier incidente que comprometa la red corporativa, además de resolverlo debemos ser mucho más ambiciosos, debemos pensar en medidas preventivas, no sólo paliativas.

- Teniendo visión de futuro. Implantando nuevas tecnologías.
- Siendo cautos. Hagámoslo en un entorno inicialmente controlado.
- Estando en permanente comunicación con el colectivo afectado. No sólo informo, sino que intento convencer para la causa.

Y en el día a día, por la responsabilidad que nos compete, y una vez comprobado el riesgo que se está generando, podríamos decir que son tres los pasos a dar:

- Primero, informe y explique, pero no pierda demasiado tiempo.
- Segundo, encomendándose a Dios, desconecte.
- Tercero, vuelva a conectar con todas las de la ley.

Sabiendo de antemano todo el ruido de fondo que se puede generar, las opiniones contrarias que se van a argumentar y las llamadas de nuestros mayores que vamos a recibir.

Eso sí, siempre nos quedará la satisfacción de haber ejercido correctamente nuestra responsabilidad y no habernos amedrentado en su ejecución, y también la perplejidad de que en lo que en otras disciplinas genera elogios en ésta genera recelos. Pero es lo que hay y con ello siempre tenemos que contar. ■

> Alicia Matarranz Relaño
Gerente de Seguridad
de Sistemas Internos TI
INDRA