Tendencias:

Transformación digital cibersegura

La mayoría de las empresas en Chile y la región están en la primera etapa de la transformación digital y, según la consultora internacional IDC, la ciberseguridad es indispensable para tener éxito en esa tarea, solo que las empresas no tienen aún conciencia de ello.

Efectivamente, como señala el director ejecutivo del Centro de Estudios del Futuro, CEF, de la USACH, Juan Luis Núñez, "uno de los mayores desafíos para las empresas es que sus máximos ejecutivos tomen conciencia de la relevancia que este tema tiene para el negocio, pues ya dejó de ser un problema de carácter técnico y se transformó en un problema del cual depende el prestigio y la vida de la compañía"; lo mismo que la transformación digital.

César Pallavicini, gerente general de Pallavicini Consultores, explica que transformar digitalmente una empresa es sinónimo de automatizar los procesos que hoy se hacen de forma compleja y manual: "El principal desafío ahí es no aumentar los riesgos de fraudes o robos de información, ya que con la forma de procesamiento actual las pérdidas económicas de las empresas por ciberataques son millonarias", precisa el ejecutivo.

IDC ratifica lo anterior. En Latinoamérica, las pérdidas económicas asociadas al cibercrimen ascienden a 90 mil millones de dólares anuales.

Para Marcelo Díaz, gerente general de Makros, "cualquier proceso de transformación digital debe tener dentro de sus ejes principales la ciberseguridad. No es posible concebir este proceso sin incluirla dentro de la discusión. Hoy más que nunca los activos digitales son fuentes permanentes de ataques y de exposición", afirma.

ESTRATEGIA

Lo evidente, dicen los expertos, es que sin seguridad no es posible avanzar hacia las nuevas tecnologías o tendencias, es decir, hacia los cambios que implica la transformación digital.

De ahí la importancia de una estrategia de ciberseguridad adecuada a la transformación digital. "La estrategia debe ser de largo plazo y con directrices y aprobaciones desde la alta dirección. El gran proyecto de transformación digital tiene que incluir la participación activa del OSI, Oficial de Seguridad de la Información, y/o del gerente de ciberseguridad. Y todo proceso de transformación digital debe, además, ser tratado en el comité de riesgo operacional de la empresa", explica César Pallavicini.

Para el experto del CEF, Juan Luis Núñez, esa estrategia debe tener como punto esencial el cuidado de los intereses de los clientes, ya sea que se trate de dinero (en el caso de la industria financiera) o datos personales (en la mayoría de las industrias), pues ello empujará una ventaja competitiva respecto al resto de los actores del respectivo sector.

"Teniendo esto como hilo transversal, resulta relevante asegurar al máximo los procesos internos en la compañía y toda la interacción con terceros, puesto que ahí puede haber siempre un punto vulnerable que sea susceptible de ataque", comenta Juan Luis Núñez.

Marcelo Díaz, de Makros, cree que, además, "se deben tener en cuenta las normas y leyes de cumplimiento que afectarán directamente a los datos, así como abordar temas como BYOD y cómo se analizarán los incidentes asociados".

RECOMENDACIONES

Junto con abordar la transformación digital, los especialistas coinciden en que es clave desarrollar al menos un Sistema de Gestión de Seguridad de la Información (SGSI ISO27001), norma ISO internacional, ya que en Chile solo hay 120 empresas certificadas.

"Los ciberdelincuentes siempre se adelantan a las empresas y atacan los nuevos desarrollos o proyectos tecnológicos de vanguardia, que son los más vulnerables", enfatiza Pallavicini.

De igual forma resulta clave que exista una convicción interna acerca de la relevancia de la ciberseguridad en la subsistencia y crecimiento de la compañía, lo cual implica ejecutar acciones que generen un cambio cultural dentro de la organización. También, agrega Juan Luis Núñez, se debe invertir en tecnología que otorgue los máximos estándares de seguridad a los clientes, pues ello genera confianza en los consumidores: "Resulta fundamental estar controlando constantemente los procesos internos a fin de detectar lo más pronto posible cualquier indicio de ataque", aconseja.

Por último, Marcelo Díaz recomienda apuntar a un modelo de seguridad en el que se entienda que ya no existe un perímetro como tal, y que se puedan aplicar los controles donde se originen, consulten o accedan los datos. "Una buena estrategia es considerar la implementación de un CASB (Cloud Application Security Broker), que permitiría tener un mayor gobierno de la ciberseguridad y de los procesos de transformación", concluye.

De acuerdo a datos de la consultora internacional IDC, el 35% de las grandes empresas en el mundo contará con un liderazgo que les permitirá transformar su estructura TI para hacer frente a la transformación digital, el próximo año. En ese escenario, la ciberseguridad es clave.

DIOMEDIA

¿Qué tan fácil es hackear un dispositivo IoT?

POR RICARDO CÉSPEDES,
gerente senior deciberseguridad de EY

A medida que nos movemos a un mundo cada vez más digitalizado, debemos reflexionar sobre cómo aparecen nuevas amenazas que pueden afectar desde temas tan simples como un sobreconsumo eléctrico por alteración del sistema automatizado de una casa, hasta situaciones de riesgo de vida por ataque a los sistemas interconectados en vehículos autónomos o dispositivos médicos.

Los dispositivos vinculados al Internet de las Cosas (IoT, su sigla en inglés) poseen diversas funcionalidades y están cambiando la forma en cómo la tecnología se integra en los ámbitos personales, de negocios y de los gobiernos, ofreciendo múltiples capacidades relacionadas a la automatización, la salud personal, monitoreo de procesos, ciudades inteligentes y el transporte público, entre otros aspectos. Para 2020, se espera que 50 mil millones de dispositivos estén conectados a internet, donde el 80% de éstos se comunicará entre sí y no a través de las personas, lo cual representa diversos desafíos desde la mirada de los riesgos que surgen.

¿Qué tan fácil es hackear un dispositivo IoT? No es tan complejo, dado que se trata de dispositivos que, en general, no se diseñaron con capacidades de seguridad que permitan protegerlos. En muchas ocasiones, los controles de seguridad son básicos o inexistentes, el control de calidad y revisión del software es nulo, la disponibilidad de actualizaciones es muy limitada y las interfaces y protocolos de comunicación no se encuentran estandarizados. Estas situaciones dejan brechas para los atacantes y complican la posibilidad de tomar acciones correctivas una vez que salen al mercado.

Con tantos dispositivos la probabilidad de un ataque es muy alta, tanto así que Gartner predice que el 25% de los ataques en 2020 se originará por medio de dispositivos IoT. En muchos casos,se parte por un ataque directo al hardware identificando puertos expuestos, lo que permite realizar un proceso de ingeniería inversa y obtener características del dispositivo, como contraseñas por defecto, que luego pueden servir en cualquier otro dispositivo de iguales características.También se pueden explotar las interfaces de administración y programación que tengan vulnerabilidades y servicios inseguros en ejecución, y monitoreo de transmisiones —que salen y llegan del dispositivo— que contengan información confidencial.

Las principales preocupaciones actuales están por el lado de la privacidad, pero no es el único punto a considerar. También se deben tomar en cuenta los aspectos legales, regulatorios y de estandarización para generar un entorno confiable y seguro. Las estrategias para lograr esto parten por manejar credenciales de acceso únicas para cada dispositivo, actualizaciones periódicas, conectarlos en redes aisladas y usar fabricantes reputados. Adicionalmente, se deben realizar evaluaciones de riesgo, controlar el ciclo de vida de los dispositivos, ejecutar pruebas de vulnerabilidad y, finalmente, mantener un monitoreo con uso de técnicas especializadas que incluyan analíticas de datos para aumentar la capacidad de detección de actividad maliciosa.

El IoT es algo inevitable, por lo que debemos activamente adecuarnos para enfrentar este nuevo entorno maximizando los beneficios que nos ofrece esta nueva tendencia, salvaguardando nuestra privacidad y garantizando las operaciones.