

CRYPTO MAGAZINE

Nº 1 | 2018

Hemos abierto
el camino para
el crecimiento





Estimada lectora,
estimado lector:

Desde la publicación del último número han ocurrido varias cosas: en el ínterin, Crypto AG ha dividido el negocio nacional e internacional en dos nuevas sociedades: Crypto International AG y Crypto Schweiz AG.

¿Cuáles son las ventajas? Con estas nuevas estructuras podemos responder mejor a las diferentes necesidades de los clientes suizos e internacionales y expandir nuestras prestaciones para el mercado con un mayor enfoque en las necesidades del cliente. Los detalles al respecto se explican en las páginas siguientes.

Además, en esta entrega mostramos en qué gran medida los países y las organizaciones civiles y militares dependen de la tecnología de la información y la comunicación (ICT). Sin estos sistemas, cada vez más interconectados en red, ya casi no están en condiciones de funcionar.

¿Qué exigencias plantean las organizaciones estatales y los ejércitos a la ICT? ¿Y qué desafío supone esta «interconexión en red del mundo» para la seguridad de la información? En esta edición de CryptoMagazine encontrará más información sobre estos temas.

Giuliano Otth
CEO
Crypto Schweiz AG

Anders Platoff
CEO
Crypto International Group AB

3 | **TEMA**

Crypto AG se prepara para crecer

6 | La tecnología de la información y la comunicación como factor de eficiencia

9 | Seguridad a la cuarta potencia: recorriendo el mundo de los datos en red

12 | Los ejércitos necesitan sistemas ICT a prueba de crisis

14 | **ENTREVISTA**
Asegurar la integridad en todo momento

18 | Estonia: el ejemplo digital a seguir

22 | **HISTORIA DE ÉXITO**
Un puesto de trabajo de alta seguridad como base para el trabajo eficiente de la policía

Pie de imprenta

Revista publicada dos veces al año | **Tirada** | 3.750 ejemplares (alemán, inglés, francés, español, ruso, árabe)

Editorial | Crypto International AG & Crypto Schweiz AG, Zugerstrasse 42, 6312 Steinhausen, www.crypto.ch

Directora de redacción | Anita von Wyl, Crypto Schweiz AG, T +41 41 749 77 22, F +41 41 741 22 72, anita.vonwyl@crypto.ch

Reproducción | Sin honorarios con el consentimiento de la Oficina de Redacción, pedido de ejemplares justificativos, Copyright Crypto International AG & Crypto Schweiz AG

Fotografías | Crypto AG: portada, S. 2, 3, 4, 5 | Getty Images: S. 9 | Jean-Paul Theler: S. 15 | Shutterstock: S. 6, 10, 12, 16, 20, 21 | Grisha Bruev/Shutterstock: S. 18 | Maciej Bledowski/Shutterstock: S. 8

Tema



Crypto AG se prepara para crecer

Crypto AG está dividiendo su negocio nacional e internacional en dos nuevas empresas. El negocio internacional será adquirido por el empresario de seguridad cibernética Andreas Linde, quien tiene una gran experiencia en este campo, y lo seguirá desarrollando Crypto International Group. La empresa suiza, Crypto Schweiz AG, será adquirida por su dirección, al frente de la cual se encuentra desde hace tiempo Giuliano Otth, director ejecutivo de Crypto AG, a través de una operación de «management buyout» (adquisición por la dirección) que incluye a la anterior empresa hermana InfoGuard AG.

CryptoMagazine se ha reunido con el propietario del Grupo Crypto International, Andreas Linde, con el copropietario y director ejecutivo de Crypto Schweiz AG, Giuliano Otth, y con Anders Platoff, director ejecutivo de Crypto International Group, para hablar sobre cómo se preparan para el crecimiento de sus nuevos negocios especializados.

¿Por qué decidieron separar el negocio suizo y el internacional de Crypto AG?

Giuliano Otth: Teníamos dos modelos comerciales con necesidades muy diferentes de los clientes en Crypto AG. Separarlos es el paso lógico para permitir que cada uno de ellos alcance su máximo potencial. En particular, esto nos permitirá responder mejor a las diferentes necesidades de nuestros clientes suizos e internacionales, desarrollando cada oferta de mercado de forma más específica. Esta operación fortalecerá a ambas empresas y a ambos grupos de clientes.

¿Qué significa esta nueva estructura de propiedad para los clientes?

Giuliano Otth: La división operativa en dos nuevas empresas se implementará en el transcurso de 2018. Con la nueva estructura de propiedad, cada empresa podrá concentrarse en su modelo de negocio, y cada una podrá realizar inversiones específicas en futuras tecnologías y canales de venta. El negocio suizo y el internacional mejorarán gracias a la expansión de sus respectivas ofertas de mercado. ¡Nuestros clientes notarán que nuestros productos satisfacen aún mejor sus necesidades!

¿Por qué eligieron a Andreas Linde para dirigir el negocio internacional?

Giuliano Otth: Andreas Linde es un verdadero emprendedor y un fuerte socio estratégico con una gran experiencia en el sector de la seguridad de la información. Queremos cooperar estrechamente en el futuro, en particular en el desarrollo de



productos. La nueva empresa Crypto International AG, una subsidiaria de Crypto International Group AB, adquiere todas las relaciones internacionales de cliente y desarrollará su oferta orientándola hacia las soluciones más completas de seguridad cibernética, además de la cartera de productos ya existente en el sector de los sistemas de cifrado de alta seguridad. Su visión del negocio, así como su sólida experiencia en el sector, convierten a Andreas Linde en la persona adecuada para mantener y desarrollar el negocio internacional.

¿Por qué eligió hacerse cargo del negocio internacional?

Andreas Linde: Los empleados de Crypto International, al igual que los de Crypto Schweiz, tienen un know-how único que no se puede encontrar en ningún otro lado. La combinación de una cartera de productos y servicios de última generación, así como una excelente base de clientes a escala global hacen que este negocio sea extremadamente atractivo. La marca Crypto es sinónimo del máximo nivel de alta seguridad y de respeto por la privacidad y la opinión de nuestros clientes, ya sea positiva o de necesidad de mejora. Estos son valores de los que me enorgullezco. Después de algunas semanas en el cargo, este sentimiento ha crecido aún más en mí. Aportamos lo mejor de la fuerza innovadora sueca y la ingeniería suiza para proporcionar a nuestros clientes la mejor seguridad cibernética.

¿En qué áreas hará otras inversiones?

Andreas Linde: El negocio internacional seguirá ampliando su oferta de criptografía y desarrollará una cartera integral de ciberseguridad, a medida de las necesidades cada vez más complejas de nuestros clientes internacionales en este campo. Zug, Suiza, seguirá siendo la sede estratégica de know-how de I+D a largo plazo del grupo. Este año queremos abrir una segunda sede de I + D en Lund, Suecia. Aspiramos a crear una

empresa de seguridad cibernética verdaderamente internacional. El grupo será dirigido por Anders Platoff, un ejecutivo con gran experiencia.

¿Cuál es su visión para el negocio internacional?

Andreas Linde: Hemos comenzado un nuevo y apasionante viaje en una actividad comercial de casi 100 años de antigüedad que se inició en Suecia en los años 1920, cuando el ingeniero textil Arvid Damm fundó una empresa sueca de criptografía. Unos años más tarde, Boris Hagelin, otro sueco bien conocido, adquirió el negocio, y transformó con éxito la pequeña empresa en un líder mundial en la industria de cifrado. Crypto AG ha liderado los avances del sector desde entonces. Ahora ha llegado el momento de iniciar la próxima era en la historia de Crypto AG, y para ello estamos alineando su identidad suiza con sus raíces suecas y dando un gran salto en el mundo de la seguridad cibernética. El negocio internacional seguirá ampliando su oferta de criptografía y desarrollará una cartera integral de ciberseguridad, a medida de las necesidades cada vez más complejas de nuestros clientes internacionales en este campo. La fusión de nuestra experiencia única en alta seguridad y seguridad cibernética es muy valiosa para nuestros clientes, que comprenden el verdadero valor de proteger contra los ataques a sus países y sus ciudadanos.

Anders Platoff: Estamos trabajando intensamente para desarrollar la próxima generación de soluciones integrales de ciberseguridad, a fin de garantizar que nuestros clientes se sientan seguros, tengan un mejor control y estén preparados para las nuevas ciberamenazas. Esperamos lanzar nuestra primera propuesta de seguridad cibernética a finales de 2018. Sin embargo, instamos a todos nuestros clientes a que se pongan en contacto con nosotros si tienen requerimientos

«Observamos un fuerte crecimiento en ciberseguridad. Con estas dos empresas de reciente creación podemos ocupar una posición de liderazgo en nuestros mercados centrales.»

urgentes o específicos en el campo de la seguridad cibernética. Haremos todo lo posible para tener en cuenta sus ideas y necesidades.

¿Cuáles son las buenas noticias de Crypto Schweiz AG para los clientes suizos?

Giuliano Otth: Con más de 150 empleados, el grupo recientemente creado con Crypto Schweiz AG e InfoGuard AG es la mayor empresa suiza de ciberseguridad. Además de nuestros conocidos sistemas de cifrado de última generación, también ofrecemos a nuestros clientes la gama completa de soluciones y servicios de seguridad cibernética, que también se adaptarán más a las necesidades de Suiza. En el futuro, los conocimientos especializados sobre seguridad, que hemos acumulado a lo largo de décadas, también estarán disponibles para las aplicaciones de IoT. De esta forma, queremos asumir un papel de liderazgo como proveedor de servicios para nuestros clientes y también como socio tecnológico para empresas de otros sectores.

Entonces, mirando hacia el futuro, entendemos que es mucho lo que los clientes pueden ganar. ¿Podría haber algún impacto negativo para los clientes en la fase de transición?

Anders Platoff: Queremos hacer todo lo posible para que la transición sea lo más fluida posible para nuestros clientes. La idea misma de esta transición es proporcionar un mejor servicio a nuestros clientes en el futuro. Sin embargo, sabemos que siempre hay dificultades para avanzar en una fase de transición, y queremos hacer todo lo posible para garantizar que no haya inconvenientes para nuestros clientes.

Giuliano y yo estamos aquí para resolver rápidamente cualquier problema que nuestros clientes puedan encontrar durante la transición.

¿En qué áreas cooperan las dos nuevas empresas y se benefician mutuamente?

Giuliano Otth y Anders Platoff: Ambas empresas desean mantener una estrecha relación y trabajar juntas en el futuro. Tenemos la intención de cooperar estrechamente en el desarrollo de los productos de Crypto. Ambos queremos ofrecer toda la cartera de productos de Crypto, aunque el enfoque será ciertamente diferente, adaptado a las necesidades respectivas de cada mercado.



Andreas Linde

El empresario Andreas Linde es el propietario y presidente del Consejo de Administración de Crypto International AB Group con sede en Lund, Suecia. Linde tiene una larga trayectoria en el sector de la seguridad cibernética. A finales de 2015, fundó la empresa Famco, que, como proveedor de servicios externos para organizaciones gubernamentales, realiza proyectos llave en mano con un núcleo de seguridad cibernética.

Hasta 2015 Andreas Linde era director general de la empresa sueca Advenica, fundada por su padre a principios de los años 90. Hoy es el mayor accionista de Advenica. Advenica ofrece diferentes soluciones de seguridad cibernética certificadas para organizaciones gubernamentales y de infraestructura crítica. En 2000 Andreas Linde también fue uno de los fundadores de 4C Strategies, una empresa que ayuda a los clientes a crear y desarrollar habilidades en gestión de riesgos, gestión de crisis y gestión de continuidad del negocio.

Andreas Linde es un emprendedor entusiasta, que trabaja movido por el impulso de crear empresas con éxito comercial a largo plazo. Posee una amplia experiencia en las áreas de ciberseguridad, seguridad de la información y desarrollo de negocios dentro del sector.

Andreas Linde tiene 43 años, está casado y es padre de dos hijas de 3 y 4 años.

La tecnología de la información y la comunicación como factor de eficiencia

El Estado, la economía y la sociedad están fuertemente influenciados por la tecnología de la información y la comunicación (ICT). En las últimas décadas, los avances de esta tecnología han demostrado ser impulsos para la modernización de las autoridades y sus procesos. Para poder seguir el ritmo del desarrollo tecnológico y también para beneficiarse de él, se necesita una estrategia que tenga en cuenta la seguridad de la información.

Un mundo sin sistemas informáticos es inimaginable hoy en día. En nuestra vida cotidiana, cuando falla un sistema es cuando notamos claramente la fuerte influencia de la tecnología de la información y la comunicación en el presente. Si, por ejemplo, no funcionan los terminales de pago en los comercios, se forman largas colas frente a las cajas. Si en un cruce de calles falla el control de los semáforos, el tráfico puede detenerse por completo durante un tiempo.

Las fallas y perturbaciones tienen diferentes grados de gravedad en sistemas con un nivel más alto de necesidad de protección. Cuanto más crítico es un sistema para el funcionamiento de procesos, más claramente muestra su falla la dependencia del Estado, de la economía y la sociedad de la tecnología de la información y la comunicación, o ICT, por sus siglas en inglés. La banda cubre desde los procesos administrativos de las autoridades o las máquinas de producción industrial hasta los sistemas informáticos para el control en centrales nucleares.

La penetración de la ICT en expansión

En los últimos años y décadas, la importancia de los sistemas de ICT ha crecido continuamente. El tema surgió por primera vez a finales de los años 70 y comienzos de los 80, cuando en el sector de las telecomunicaciones se empezaron a transmitir informaciones digitales a una mayor escala. Con la transmisión de informaciones digitales, la tecnología de la información tradicional y la tecnología de la comunicación comenzaron a aproximarse entre sí. Entre tanto, estas dos tecnologías, que antes estaban separadas, hoy se han fusionado de manera irrevocable.

La ICT comprende esencialmente tres funciones básicas diferentes:

- la comunicación, es decir, la transmisión de información de un lugar a otro,
- el almacenamiento de la información, o sea, en realidad, la captura real de datos de un momento hasta otro momento posterior, así como
- el procesamiento de la información, es decir, la transformación de los datos según unas reglas definidas. Esto último podría denominarse comúnmente cálculos computacionales.

Para el Estado, la economía y la sociedad, la tecnología de la información y la comunicación es esencial. Sin sistemas de ICT simplemente no podrían funcionar. Con el paso del tiempo, la dependencia ha aumentado claramente, en paralelo a la conexión en red de los sistemas individuales, que es cada vez más intensa. Las ventajas de la conexión en red son evidentes: los procesos se simplifican y aceleran. Con ello, la ICT ha contribuido esencialmente a la modernización de todos los ámbitos de la vida.

La ICT impulsa la modernización

En organizaciones y en el entorno de los poderes públicos, la ICT ha influenciado en muy gran medida el diseño de los

procesos en sí. Incluso las acciones más simples ya no pueden ejecutarse sin sistemas técnicos. Una gran parte de las informaciones se conserva hoy con tecnología exclusivamente digital. Y, por tanto, los datos solo pueden leerse y procesarse con ayuda de los instrumentos adecuados. La dependencia se refuerza por el hecho de que la cantidad de los datos que se capturan, transportan, almacenan y procesan ha aumentado enormemente. El procesamiento y la transmisión de los volúmenes de datos usuales actualmente son impensables sin la ICT. En contrapartida, es precisamente la ICT actual la que ha hecho posible estos grandes volúmenes de datos.

No existen señales ni razones para pensar que el desarrollo tecnológico vaya a ralentizarse o incluso acabarse. Al contrario: la tecnología de la información y la comunicación posiblemente seguirá siendo un motor determinante para la modernización que continuará en el futuro. Palabra clave: transformación digital. En este entorno, es imperativo que las empresas, las organizaciones y las autoridades públicas piensen y planifiquen bien el uso de la ICT.

En Suiza, los primeros impulsos para planificar el tratamiento de la ICT datan de 1998. La ICT se consideró un medio importante para aumentar el bienestar de forma sostenible. Desde entonces se han formulado dos estrategias informáticas. Actualmente Suiza se encuentra en pleno proceso de implantación de la estrategia (2016 – 2019), cuyo objetivo es conformar a

largo plazo la ICT de la Confederación de forma más orientada a la economía, más integral, más fiable y más enfocada.

Es imperativo que las empresas, las organizaciones y las autoridades públicas piensen y planifiquen bien el uso de la ICT y tengan en cuenta la seguridad de la información.

La visión prescribe las medidas

Una estrategia de ICT es también indispensable bajo el punto de vista de los costos. Es cierto que las tecnologías modernas y la automatización de los procesos han contribuido significativamente a que las secuencias y procesos en las administraciones públicas sean más baratos y rápidos. Sin embargo, la ICT también ha creado al mismo tiempo la necesidad de recopilar y evaluar ciertos datos. El resultado de esta nueva situación es la enorme cantidad de datos que se deben procesar, almacenar y mantener, así como una gran cantidad de interfaces que deben ser administradas y vigiladas. De hecho, el costo de la ICT es y sigue siendo un factor clave, a pesar de que el desarrollo



tecnológico ha llevado a una disminución constante de los precios de la infraestructura física para el procesamiento, la transmisión y el almacenamiento de datos e información.

En vista del costo de implementar proyectos de ICT y del costo, que tampoco debe infravalorarse, de funcionamiento de aplicaciones de ICT, la eficiencia y la rentabilidad son componentes clave de cualquier estrategia de ICT. El objetivo siempre es tener una visión integral, es decir, la rentabilidad y la eficiencia deben evaluarse desde la perspectiva general. Además, para evaluar los costos, es importante realizar un seguimiento no solo de la duración de un proyecto, sino de los gastos que probablemente surgirán durante la vida útil de un sistema.

Tener en cuenta todas las exigencias

Sin embargo, además de la eficiencia y la rentabilidad, existen muchos otros aspectos que merecen al menos la misma atención en una estrategia de ICT. Uno de ellos podría describirse como conveniencia. Es importante asegurarse de que la ICT siempre esté alineada con las necesidades de una unidad administrativa u organizativa y las respalde en la prestación de sus servicios. Deben tenerse en cuenta las exigencias de los usuarios, así como las de otras partes interesadas, a saber, los ciudadanos, los destinatarios y proveedores externos de servicios, además de otras autoridades. El conflicto de intereses es inevitable: Si por consideraciones de costo y practicidad, se buscan en lo posible soluciones de ICT estandarizadas, las necesidades específicas de las unidades administrativas individuales no se podrán satisfacer por completo. Las soluciones demasiado unificadas también conllevan el riesgo de que la ICT ya no pueda desempeñar su papel de motor impulsor de la eficiencia.

En las estrategias de ICT se debe prestar especial atención a la seguridad de la información. Esta es la clave para asegurar el funcionamiento continuo y sin problemas de los sistemas y garantizar la seguridad del Estado. La seguridad de la información es uno de los factores de éxito críticos, el cual también se debe tener en cuenta en la gestión del riesgo. Los efectos de un fallo del sistema, de la pérdida de datos o incluso del robo de datos pueden, en última instancia, ser graves.

Aunque el tamaño de los riesgos siempre depende de los organismos involucrados, una negligencia en el área de la seguridad de la información puede ser francamente devastadora para un Estado en muchos ámbitos. Por lo tanto, es importante dar el alcance necesario a los temas relevantes ya en la estrategia para abordar la ICT. Cuando se trata de salvaguardar la confidencialidad y la integridad de los datos, es decir, la protección contra el acceso y la alteración no autorizados, la eficiencia ya no debe ser el criterio más importante.

Tras una caída de tensión el control del tráfico debe estar garantizado



Seguridad a la cuarta potencia: recorriendo el mundo de los datos en red

El mundo avanza rumbo a la hiperconexión en red. A medida que la penetración de la tecnología de la información aumenta, también lo hace la necesidad de protección de los sistemas subyacentes, así como de las informaciones digitales circulantes. La tecnología Crypto SmartProtect tiene en cuenta esta evolución. Permite operar hasta cuatro zonas de seguridad completamente aisladas en un dispositivo, de modo que los datos confidenciales estén protegidos de forma integral en todo momento.

La información y las personas viajan hoy más rápido que nunca. Muchas aplicaciones y campos de actividad ya se han liberado de sus raíces locales y se han desplazado al ciberespacio. Debido a los peligros que acechan allí, es imperativo que los sistemas de la tecnología de la información y la comunicación (ICT) estén diseñados de tal manera que los componentes, procesos, interfaces e información de relevancia crítica para la seguridad estén protegidos de manera fiable en todo momento.

El cambio permanente aumenta la vulnerabilidad

La ICT moderna ofrece un gran potencial para la estandarización. Este potencial se debe aprovechar de forma lógica en la medida de lo posible, por ejemplo, según la estrategia de ICT de la Confederación Suiza. No hace falta decir que debido a la diversidad de áreas especializadas en el entorno de los poderes públicos, es imposible alcanzar una estandarización general. Por ejemplo, actualmente se utilizan en Suiza hasta 6.000 aplicaciones especializadas diferentes. Estas necesidades

específicas de diferentes partes interesadas deben satisfacerse. Para empeorar las cosas, la cantidad de sistemas y dispositivos conectados en red aumenta constantemente, y las consecuencias de ello difícilmente pueden estimarse hoy. Una cosa está clara: la digitalización ha aumentado la vulnerabilidad general. Incluso Gobiernos y organizaciones con una protección informática bien desarrollada han sido víctimas de ciberataques en el pasado reciente. En muchos casos, los atacantes pudieron utilizar componentes de infraestructura mal configurados o vulnerabilidades identificadas demasiado tarde, para obtener acceso a datos sensibles.

Garantizar la seguridad operativa combinada con la máxima facilidad de uso es un desafío clave que debe abordarse. También se debe tener en cuenta que las estructuras de internet están sujetas a cambios permanentes. A un ritmo rápido, los avances tecnológicos están abriendo nuevas posibilidades de aplicación que deben integrarse en las infraestructuras informáticas existentes. En un futuro cercano, es probable que se agreguen componentes informáticos externos, como el Internet de las Cosas (IoT, en inglés). Además, la recopilación e interconexión de grandes cantidades de datos (big data) abren posibilidades hasta ahora desconocidas.

Garantizar la seguridad operativa combinada con la máxima facilidad de uso es un desafío clave que debe abordarse.

Eliminar los riesgos de seguridad

El amplio uso de las tecnologías móviles ya se ha generalizado. Hoy en día ya no es posible trabajar de manera eficiente sin utilizar dispositivos móviles. La conexión en red segura de los sistemas fijos y portátiles se ha convertido en uno de los factores de éxito más importantes. Pero para ello se debe disponer de infraestructuras de ICT que permitan y aseguren una comunicación sin restricciones y una cooperación total: comunicación y colaboración unificadas, o Unified Communication and Collaboration (UCC, en inglés). Los usuarios necesitan acceder a sus datos y documentos en todo momento y en cualquier lugar: ya sea esta información pública o sujeta a confidencialidad. Es importante prestar especial atención a esto, especialmente si los datos sensibles deben compartirse en una red o con socios individuales según la situación.

Un ejemplo: si un ciudadano de un Estado es secuestrado en el extranjero, el Ministerio de Relaciones Exteriores del país de origen del secuestrado suele ser el encargado de encontrar una solución. En algunos casos, una operación de este tipo requiere recurrir a instrumentos que no están vinculados al Ministerio de Relaciones Exteriores. Por ejemplo, asesores externos o unidades policiales. Para garantizar que el intercambio de



Trabajo fácil para el usuario en un dispositivo

información en esta red funcione de manera segura, se requieren tecnologías compatibles con el tráfico paralelo de datos.

Lo mismo se aplica a las operaciones con participación militar: por ejemplo, los militares llevan a cabo misiones subsidiarias, para cuyo éxito es determinante el intercambio seguro de datos. Al mismo tiempo, es crucial que el mando del ejército tenga acceso a canales de información interna, por un lado, y, por otro lado, que el intercambio de información con las otras partes involucradas funcione de manera impecable y segura.

En tales constelaciones generalmente también se intercambian informaciones con diferentes niveles de clasificación. Por lo tanto, este intercambio necesariamente debe hacerse a través de redes completamente independientes unas de otras, porque solo la separación consecuente asegura la más alta seguridad de la información. Durante mucho tiempo esto fue posible solo mediante el uso de varios dispositivos. Esta ya no es la práctica común hoy en día. Por un lado, porque contradice las necesidades actuales de los usuarios y, por otro lado, porque demanda un tiempo valioso.

Hasta cuatro entornos de usuario con una estación de trabajo

Con la tecnología Crypto SmartProtect, se superan los obstáculos mencionados. Ella permite el procesamiento seguro de la información en un solo dispositivo. El usuario tiene la posibilidad de trabajar con hasta cuatro zonas de seguridad completamente aisladas (Compartments). Con los dos Compartments estándares, se puede, por un lado, acceder a internet (nivel de clasificación: información pública). Por otro lado, el segundo Compartment ejecuta las aplicaciones que se requieren para el procesamiento de la información interna (nivel de clasificación: información interna). Además, la tecnología Crypto SmartProtect también hace posibles soluciones con más Compartments: un tercer Compartment para documentos confidenciales (nivel de clasificación: confidencial) y un cuarto Compartment para datos y aplicaciones clasificados como secretos (nivel de clasificación: información secreta).

Dependiendo de las exigencias, se pueden definir diferentes restricciones para los Compartments. Por ejemplo, sin conexión a impresoras o sin utilización de memorias USB para el nivel de clasificación secreta (cuarto Compartment). En el segundo Compartment, sin embargo, estas opciones están

disponibles para el usuario. La ventaja de esta solución es que el usuario puede trabajar en su entorno de usuario conocido y en una situación de crisis no tiene que acceder a un sistema que se use rara vez.

Los terminales en el punto de mira

Saber lo que se necesita para cumplir con las exigencias de seguridad es una cosa: actuar en consecuencia, otra. Sin embargo, cuando los empleados tienen terminales que les permiten moverse en entornos de usuario habituales en zonas de seguridad aisladas unas de otras, los riesgos para la información confidencial se eliminan de manera consecuente. Esto es importante en la medida en que recientemente los terminales han estado en el punto de mira de los hackers y han sido utilizados como «trampolines» para penetrar en otros niveles de un sistema informático.



Los ejércitos necesitan sistemas de ICT a prueba de crisis

En la era digital, es más importante que nunca para los ejércitos garantizar que su soberanía permanezca intacta. La fiabilidad, la integridad y la disponibilidad de los canales de comunicación deben estar sujetas a un control sin fisuras. Garantizar esta seguridad de los sistemas de ICT es un desafío cada vez más importante, ya que resulta esencial para la disponibilidad.

Un ejército debe ser operativo y estar disponible en todo momento y en todas las situaciones. Aquí, la comunicación dentro de la tropa y la transmisión segura de las informaciones desempeñan un papel decisivo. El apoyo a los mandos a través de los modernos recursos informáticos es cada vez más importante. Especialmente en situaciones de crisis, la comunicación confidencial debe funcionar. Bajo ninguna circunstancia la información confidencial debe caer en las manos equivocadas o ser manipulada. La información y los informes de situación deben permanecer confidenciales incluso años después de una misión.

Debido al rápido desarrollo tecnológico, la densidad de la información y sus necesidades de disponibilidad van en aumento. Con la mayor disponibilidad crecen también las exigencias de seguridad de la información. Especialmente los sensores y efectores en el campo (por ejemplo, drones, cámaras corporales o radares) suministran hoy en día una información con imágenes de alta resolución que requiere una mayor anchura de banda en los sistemas de transporte. En el campo táctico, se pueden utilizar modernas radios IP, la comunicación

satelital o la comunicación móvil militar 3G o 4G. Las estructuras de red fijas se basan actualmente en redes de microondas y cada vez más en cables de fibra óptica rápidos.

Hasta el momento, muchos sistemas distintos de antigua generación suelen operar en paralelo, basados en tecnologías y lenguajes de programación diferentes. Además, los datos generalmente se almacenan aislados y de forma descentralizada. El problema con la tecnología obsoleta es que, en su conjunto, proporciona muy poca integración y ancho de banda para las nuevas demandas de información integral de comando en tiempo real.

Asegurar la capacidad de actuar

Para que no se limite la capacidad de actuar de un ejército en una situación de crisis, los sistemas deben ser resistentes a los ataques externos. El endurecimiento y la protección de estas redes y centros de datos a prueba de crisis se logran mediante el endurecimiento físico y el cifrado y la protección adecuados de la información. Para el cifrado de la comunicación y el aseguramiento de las redes, Crypto International AG y

La independencia de la red militar es de suma importancia

Crypto Schweiz AG ofrecen diferentes soluciones que tienen en cuenta las necesidades de cada caso. Estas se basan en la arquitectura de seguridad de Crypto. Esto permite repeler los ataques siempre con las medidas de seguridad más fuertes disponibles. Para la conexión de sitio a sitio, los Crypto cProducts protegen la información contra los ataques durante la transmisión a nivel de la información, mediante el uso de criptografía (lógica / criptográfica).

A más tardar desde el caso Snowden se sabe que los sistemas relevantes también deberían estar separados dentro de la red troncal para lograr una zonificación de la información. Por ejemplo, el sistema de radar de las fuerzas aéreas está lógicamente/criptográficamente separado de la telefonía, del sistema de acceso biométrico y del sistema de soporte e información del mando. Esto garantiza que no se produzca ningún intercambio de información entre zonas en el caso de una falla, pero también si hay una manipulación deliberada. Finalmente, una parte de la información requiere el cifrado de extremo a extremo. Aquí se utilizan soluciones para el usuario final, en las que la voz, los documentos en papel o los documentos electrónicos se pueden transmitir de forma segura con el más alto nivel de confidencialidad.

El objetivo de un ejército es ser autónomo y no depender de proveedores civiles en situaciones de emergencia. Esta idea garantiza que, también en escenarios de crisis, las redes protegidas actúen como conexión entre el ejército y el Gobierno, así como con operadores de infraestructuras críticas (centrales nucleares o aeropuertos), para que los servicios básicos en situaciones de crisis funcionen perfectamente. A menudo, los sistemas están fuertemente interconectados entre sí para permitir una evaluación óptima de la situación y la planificación de escenarios. Para el cuadro operativo se recopila una información integral sobre una misión y se la procesa centralmente. Esto sirve para una óptima preparación, para un mando operativo efectivo y, luego, como documentación.

El ejército en el siglo XXI

Muchos ejércitos están dando el paso para ingresar al siglo XXI. Una parte esencial de la modernización es la garantía de la seguridad de los sistemas. Esto incluye la monitorización de las redes y la detección de ciberataques en sistemas de ICT y, de ser necesario, la activación de las contramedidas necesarias

Además de los nuevos centros de datos, a menudo se deberá establecer una red de telecomunicaciones independiente que reúna los diferentes sistemas en una red. Las antiguas redes de transmisión con cable de cobre y de radioenlaces dirigidos son reemplazadas por fibra de vidrio. La transmisión cifrada de datos es posible entre muchas posiciones individuales. De esta red deberían beneficiarse no solo los ejércitos, sino también las organizaciones civiles que llevan a cabo tareas relacionadas con la seguridad. Gracias a las soluciones de Crypto International AG y Crypto Schweiz AG, es posible compartir incluso aquellas infraestructuras que, sin embargo, se puedan operar al mismo tiempo con alta seguridad y separadas entre sí.

Para que no se limite la capacidad de actuar de un ejército en una situación de crisis, los sistemas deben ser resistentes a los ataques externos.

A medida que se actualiza la tecnología de las redes según los últimos avances, la voz y los datos pueden transmitirse al campo desde la red de transporte fija y segura del ejército, a través de los componentes móviles y fijos, independientemente de los proveedores privados de telecomunicaciones. Otro objetivo de modernizar los sistemas de ICT es reducir el número de sistemas e introducir plataformas uniformes.

Una logística fluida es indispensable para el funcionamiento de un ejército. Los recursos limitados, tales como vehículos, suministros de tropas y avituallamiento, deben estar disponibles de manera rápida y expedita. Los centros farmacéuticos del ejército pueden asumir tareas para la población en situaciones de emergencia y ayudar a garantizar la atención médica. Estos movimientos de materiales y servicios de logística para apoyar la planificación de recursos difícilmente pueden realizarse sin un sistema informático basado en ERP. La capacidad operativa del ejército está garantizada si la logística puede proporcionar los recursos a tiempo y de forma adecuada a las necesidades. Forman parte de ello, naturalmente, la disponibilidad (planificación y suministro de los recursos), pero también un proceso logístico funcional que incluye la logística informática asociada. La conexión de este proceso a redes a prueba de crisis aumenta la disponibilidad y garantiza el proceso logístico. La tecnología de última generación y componentes de ICT endurecidos con una protección según los últimos avances técnicos garantizan aquí un funcionamiento eficiente.

«Asegurar la integridad en todo momento»

Hoy en día, las operaciones militares están respaldadas principalmente por herramientas de la tecnología de la información y la comunicación (ICT) y ya no pueden llevarse a cabo eficazmente sin ellas. Además de las muchas ventajas y oportunidades que ofrece la ICT, esta utilización también conlleva nuevos riesgos y peligros que deben abordarse de manera muy consciente en el entorno militar.

¿Qué exigencias plantea un entorno militar a la ICT?

En comparación con el entorno civil, las exigencias de robustez, disponibilidad y seguridad de la información se consideran y ponderan de forma diferente desde la perspectiva militar. El ejército debe cumplir sus tareas en todas las situaciones y teniendo en cuenta todo tipo de amenazas. Además, la ICT nunca es un fin en sí misma en el entorno militar, sino que más bien apoya a los actores militares en el cumplimiento de sus tareas y funciones. Hago hincapié en esto porque, como consecuencia de un rendimiento defectuoso o faltante de la ICT, es muy probable que se produzcan daños personales. Estos aspectos también definen esencialmente las exigencias diferentes y cada vez mayores que se plantean a la ICT en el entorno militar. En concreto, esto significa que necesitamos infraestructuras de ICT en el entorno militar, capaces de seguir funcionando en todas las situaciones, tanto tras un ataque militar como también después de grandes desastres naturales o fallos generalizados del suministro eléctrico, para que los servicios de ICT necesarios se puedan seguir utilizando.

¿En qué campos de acción están los mayores desafíos?

¿Qué estrategias considera útiles el Ejército Suizo para enfrentarse a ellos y cómo se implementan?

El Ejército Suizo tiene la misión primaria de proteger a la población suiza y garantizar la integridad de Suiza. Con esto quiero decir que está orientado a actuar en primera instancia dentro de sus propias fronteras. Esto significa asimismo que debemos proporcionar y garantizar nuestros servicios de ICT esencialmente también dentro de Suiza. Actualmente nos enfrentamos a los mayores desafíos en los siguientes campos de acción: la conexión en red segura y robusta de sistemas y actores, el aseguramiento del suministro de la información requerida en el momento adecuado y la ciberdefensa, es decir, la detección y prevención de amenazas en el ciberespacio.

Puesto que como ejército debemos prestar nuestros servicios en todas las situaciones, es decir, permanentemente, en el campo de los servicios de ICT disponemos de infraestructuras y sistemas propios, reforzados y de funcionamiento autónomo, que podemos utilizar y operar con nuestro propio personal

(personal de Defensa y miembros de la milicia). Además debemos asegurarnos de que nuestro personal tenga los conocimientos y la experiencia necesarios para realizar estas tareas de forma independiente y autónoma.

Con el programa FITANIA, estamos renovando nuestras infraestructuras de ICT y adaptándolas a las exigencias y amenazas actuales. Este programa incluye los tres grandes proyectos para la construcción de la red de comando de Suiza, la renovación de las telecomunicaciones del ejército y la construcción de nuevos centros de procesamiento de datos. Por lo demás, el Jefe del Departamento Federal de Defensa, Protección Civil y Deportes (abreviado: VBS), el consejero federal Guy Parmelin, ha aprobado el Plan de Acción de Ciberdefensa. Con su implementación se crean en el departamento las condiciones marco para que el ejército también pueda proporcionar los servicios requeridos en esta área.

El rápido progreso tecnológico requiere ajustes constantes en el ámbito de la ICT. ¿En qué punto está el Ejército Suizo en general y en comparación con otros países?

El progreso tecnológico no se detiene tampoco frente al Ejército Suizo. Sin embargo, a diferencia del mundo civil, las necesidades en el mundo militar, especialmente en Suiza, no están impulsadas por las tendencias y posibilidades tecnológicas, sino por las nuevas y cambiantes amenazas y las necesidades resultantes. Por supuesto que también en el entorno militar se emplean las nuevas tecnologías y los productos basados en ellas. Esto se hace en el sentido de la utilización de estas nuevas oportunidades para apoyar la satisfacción de las necesidades del ejército y el cumplimiento de las tareas militares.

El Ejército Suizo tiene una gran ventaja con su sistema de milicias. Nuestros soldados y los miembros del ejército crecen con los avances tecnológicos de hoy. Para ellos, la utilización de estas tecnologías y productos no es nada fuera de lo común. Por otro lado, el uso de sistemas modernos es cada vez más complejo y requiere una organización profesional fuerte y competente con especialistas que configuren, mantengan y reparen estos sistemas, para que puedan ser utilizados por la

tropa (miembros de la milicia). El gran desafío aquí es que competimos con otras grandes empresas informáticas civiles para atraer a estos especialistas en ICT de la organización profesional en el mercado laboral suizo.

La integridad y autenticidad de los datos es esencial.

La tendencia apunta en muchos casos hacia la estandarización de estructuras y procesos de ICT. ¿Esto es también aplicable al ámbito militar?

Correcto, esto también se aplica al entorno militar. La estandarización es necesaria, en particular para garantizar la interoperabilidad con los socios militares y civiles. Desde la Segunda Guerra Mundial, las operaciones militares se han llevado a cabo principalmente en conjunto con otros ejércitos o, en la gestión de eventos naturales importantes, con fuerzas operativas civiles. Para tener éxito juntos y permitir esta colaboración fue necesario encontrar un lenguaje común y definir secuencias, procesos y también interfaces. Este trabajo fue particularmente importante para la cooperación de los aliados en el mundo occidental, lo que ha llevado a un gran esfuerzo en el área de la estandarización militar de estructuras y procesos y a un gran número de estándares técnicos. Sin estandarización, el uso de las tecnologías actuales, como las tecnologías de telecomunicaciones, no sería posible. Por cierto, esto también se aplica al mundo civil.

¿Qué escenarios de amenazas excluyen de antemano la posibilidad de una estandarización general, y cuáles son los principales riesgos de los sistemas de ICT del ejército?

Básicamente, la estandarización sirve principalmente para garantizar la interoperabilidad y la cooperación. Pero con ello, también promueve la transparencia. Esto significa que un atacante potencial sabe cómo hacemos algo y, por tanto, puede planificar mejor cómo atacar y causar daños. Por otro lado, si uso un procedimiento estandarizado, por ejemplo, un protocolo específico, entonces también sé mejor dónde están los puntos débiles y los riesgos. Dependiendo de cada situación de amenaza, puedo tomar las medidas apropiadas para minimizar o incluso eliminar estos riesgos. Es importante que yo conozca los riesgos que pueden obstaculizar o incluso imposibilitar el cumplimiento de mis tareas. Conociendo estos riesgos y considerando las amenazas y los peligros a los que me enfrento, puedo tomar las medidas apropiadas para esquivar o evitar estas amenazas. Como ya se ha dicho anteriormente, los sistemas de ICT apoyan el cumplimiento de las tareas del ejército. En resumen, puede decirse que los sistemas de ICT del ejército sirven para generar, procesar, almacenar, transportar y presentar datos o información. Sobre esta base, podemos identificar básicamente dos riesgos: por un lado, el riesgo de que se pierda información, o sea, que ya no se pueda usar, y por otro



Jean-Paul Theler estudió Macroeconomía en la Universidad de Lausana. Luego obtuvo un máster en Matemática Económica por la London School of Economics and Political Science y un doctorado (oec. publ.) por la Universidad de Lausana. En 1996, Jean-Paul Theler ingresó al Cuerpo de Instrucción y se desempeñó en diferentes funciones, incluida la formación de cuadros y como responsable de la doctrina militar. Fue ascendido a brigadier como Jefe de Personal del ejército. Desde el 1 de enero de 2013 hasta el 31 de diciembre de 2017, dirigió en su división la Base de Soporte Ejecutivo y fue responsable de la prestación de servicios en el ámbito de la tecnología de la información y las telecomunicaciones, así como de las operaciones electrónicas.

En el contexto de la implementación del desarrollo posterior del ejército, es desde el 1 de enero de 2018 jefe de proyecto del Comando de Asistencia. De acuerdo con la decisión del Parlamento suizo sobre la organización del Ejército Suizo, el Comando de Asistencia reunirá las tareas actuales de la Base de Soporte Ejecutivo y la Base de Logística del ejército.



También los soldados usan cada vez más ayudas técnicas

lado, que la funcionalidad de mis sistemas se ve alterada o destruida. Estos son, concretamente, riesgos del ciberespacio:

- fugas de datos o alteración de funciones y procesos basados en software,
- fallos humanos, como la incorporación intencional de errores o puntos de ataque en el software (backdoors),
- manipulación consciente de datos y procesos,
- amenazas físicas por los elementos y fuerzas cinéticas (terremotos, explosiones, armas, etc.),
- interrupciones en el suministro de energía (electricidad o agua).

Con esto quiero mostrar que, para los sistemas de ICT del ejército, no solo son de gran importancia los riesgos en el ciberespacio, sino que también existen otros riesgos equivalentes. Esta es una diferencia significativa con respecto a la percepción de los riesgos en el entorno civil.

¿Cuál es la importancia de la seguridad de la información en términos concretos?

La seguridad de la información es sumamente importante, sobre todo, naturalmente, la protección de los datos y de la información. En el ámbito militar, el sistema de clasificación de la información – SECRETO, CONFIDENCIAL, USO INTERNO- crea una estructura que también influye en los impulsos para la gestión de la información. Las medidas para la protección de la información en el nivel SECRETO, comenzando en el plano de las infraestructuras de ICT, hasta los procesos de gestión, son más integrales y restrictivas que en el nivel de USO INTERNO.

Al mismo tiempo, la integridad y autenticidad de los datos es esencial. Las decisiones de un comandante se basan en la información que tiene a su disposición. Si, por ejemplo, un enemigo puede manipular la información, entonces una decisión también puede verse fuertemente influenciada. Como resultado, el requisito básico para la seguridad de la información es la integridad y el funcionamiento de los recursos de ICT.

Desde su punto de vista, ¿a qué amenazas específicas está más expuesta la seguridad de la información?

Desde el punto de vista del ejército se pueden distinguir las siguientes amenazas fundamentales: primero, la fuga de información, segundo, la destrucción u obstaculización del acceso a la información y, en tercer lugar, la manipulación o corrupción de la información. Al «robar» informaciones, la parte contraria desea obtener información (por ejemplo, documentos de planificación, información de acceso, como contraseñas, certificados), lo que le da superioridad en la información y le permite acceder a los sistemas informáticos para manipularlos o apropiarse de ellos. Con la destrucción u obstaculización del acceso a la información, se intenta imposibilitar el uso de los recursos del enemigo. Si, por ejemplo, se puede evitar que las imágenes de un dron de reconocimiento lleguen al centro de operaciones, puede imposibilitarse el uso de un arma. Mediante la manipulación de la información y los datos, es posible tomar otras decisiones erróneas o incluso bloquear los sistemas.

Las directrices actuales del ejército prohíben la creación de redes de dispositivos privados con las infraestructuras de ICT del ejército y la administración.

Las tecnologías como el Internet de las cosas (IoT) aún están verdes, pero en el futuro permitirán que los dispositivos se comuniquen directamente entre sí. ¿En qué punto está el ejército en relación con el IoT? Es decir: ¿dónde ve usted el mayor potencial para el IoT en el entorno militar?

El IoT es, como muchos otros temas, una exageración que no es directamente relevante en el entorno militar. Por otro lado, si se considera el tema en términos generales, es decir, la conexión en red de muchos recursos informáticos diferentes y la comunicación directa de estos recursos entre sí, esto también será ciertamente importante en el entorno militar.

En el entorno militar, en estos casos se habla de bucle sensor-efector, es decir, la conexión en red de los sensores con los efectores en un proceso más o menos automático. Hoy en día, el ser humano todavía representa en este bucle la inteligencia central y primaria y, por tanto, es el que toma las decisiones. Además, el soldado está equipado en el frente con un número cada vez mayor de sensores, los cuales transmiten los datos de forma directa y autónoma a los puestos de comando centrales. La información consolidada se transmite de vuelta al soldado, lo que permite un uso más eficiente de las armas sobre el terreno. En la tendencia de reducir la exposición del ser humano en el frente como el eslabón más vulnerable y débil, la automatización de este bucle se fortalecerá en el futuro. Sin embargo, en mi opinión es de vital importancia que, en el uso de las armas, el ser humano siempre tome la decisión final y así asuma su responsabilidad. La guerra completamente automatizada no debe convertirse en realidad.

Supongo que, al igual que en el entorno civil, el IoT como tecnología tendrá mayor importancia en el área de soporte y podría, por ejemplo, automatizar aún más los procesos logísticos.

¿Qué riesgos de seguridad enfrenta la comunicación y cómo se puede diseñar una protección efectiva?

A medida que el IoT automatice más los procesos, la seguridad de extremo a extremo se volverá más importante. Las exigencias para garantizar la autenticidad e integridad de la información se incrementan enormemente, y al mismo tiempo crece fuertemente la cantidad de posibles puntos para un ciberataque. Esto tiene que llevar a que toda la información esté empaquetada de tal manera que contenga elementos de identificación que permitan la identificación y la autenticación y, de ese modo, aseguren la integridad de la información transportada.

¿Hasta qué punto los dispositivos privados suponen un riesgo de seguridad en las operaciones militares? ¿Y qué medidas de protección toma el ejército?

Los recursos privados de ICT representan un riesgo de seguridad por sí mismos en operaciones militares porque se utilizan para las mismas actividades que los equipos militares equivalentes o similares, pero no están equipados ni se usan con las mismas medidas de protección o al menos equivalentes.

Ciertamente, al evaluar los riesgos de seguridad, es necesario diferenciar en términos del tipo de dispositivo privado y la ubicación del uso, pero, en la mayoría de los casos, estos dispositivos no se usan de forma aislada, sino que se conectan con el entorno a través de alguna infraestructura. Claramente inviable es la conexión en red de dispositivos privados con infraestructuras militares, pero incluso si se utilizan independientemente de las infraestructuras de ICT militares, suponen un riesgo de fuga incontrolada de datos. También son un riesgo como sensores no controlados, por ejemplo, a través de la función de localización en el caso de un teléfono inteligente o del micrófono o de la cámara en una computadora portátil o de un teléfono inteligente.

Las directrices actuales del ejército prohíben la conexión en red de dispositivos privados con las infraestructuras de ICT del ejército y la administración. Además, las infraestructuras de ICT están protegidas contra el acceso no autorizado a la red por diferentes mecanismos. Al acceder a instalaciones militares clasificadas, se realiza un control de ingreso y equipaje como en los aeropuertos. Pero la medida de protección más efectiva sigue siendo la autodisciplina y el control de superiores y camaradas.



Estonia: el ejemplo digital a seguir

Estonia, el pequeño Estado de Europa del Este, es considerada pionera de la digitalización. Estonia ha utilizado las nuevas posibilidades tecnológicas antes y de manera más consecuente que otros países. Aunque este camino no está exento de riesgos, Estonia se considera un modelo a seguir, también en lo referente a la protección de datos y las infraestructuras informáticas.

Estonia supo aprovechar las oportunidades. Cuando el país se independizó de la Unión Soviética en el verano de 1991, pudo crear de la nada nuevas estructuras estatales. Los jóvenes políticos que llegaron al poder reconocieron rápidamente el potencial de las nuevas tecnologías y del emergente internet. A mediados de los años noventa lanzaron una primera gran ofensiva educativa informática, en la que todas las escuelas recibieron hardware y software apropiados. El propio Gobierno trabaja sin soporte de papel desde finales de los años noventa.

Hoy Estonia ocupa el primer lugar de la Unión Europea (UE) en el ranking de digitalización de la administración. Y eso no es

de extrañar, porque casi toda la interacción entre el Estado y sus ciudadanos puede tener lugar por internet. Las únicas tres excepciones son el matrimonio, el divorcio y la compra de una vivienda, las cuales requieren presencia y firma físicas. Los estonios y estonias están aprovechando las nuevas oportunidades. Casi el 10 por ciento de los votantes votaron por internet en las elecciones europeas de 2014, y más del doble, en las elecciones parlamentarias nacionales del año siguiente. Ahora casi todos los ciudadanos del país completan sus declaraciones de impuestos por internet. Una parte importante de ellas ya se rellena automáticamente, porque las autoridades tributarias, los bancos y las empresas están conectados en red.

Además, el sector de la salud es un buen ejemplo del alto nivel de digitalización. Desde hace aproximadamente diez años, este país báltico tiene un sistema unificado de registros electrónicos de salud que almacena las historias clínicas de todos los habitantes. Tanto médicos como pacientes tienen acceso a él. La plataforma de e-salud también organiza citas médicas, lleva a cabo consultas simples y prescribe medicamentos.

Internet como derecho fundamental

Los fundamentos para hacer que todo ello funcione se establecieron alrededor del cambio de milenio. En ese momento, el Parlamento de Tallin fijó el acceso a internet como derecho fundamental en la Constitución. Y no fue solo una promesa vacía. Para cumplirla, construyó una sólida infraestructura de banda ancha que se renueva periódicamente. También la cobertura con internet móvil es excelente en este país relativamente poco poblado, con algo más de 1,3 millones de habitantes.

Según las cifras de la UE, para todos los indicadores que miden el nivel de digitalización, el país está por encima de la media europea. Por ejemplo, alrededor del 86 por ciento de las personas entre 16 y 74 años usan internet regularmente (promedio de la UE: 76 por ciento), y el 87 por ciento de los hogares tienen un acceso de banda ancha (promedio de la UE: 80 por ciento).

El Gobierno continúa invirtiendo muchos recursos en el fortalecimiento de las competencias digitales. Por ejemplo, en las escuelas, la programación es una asignatura normal. Sin embargo, el país se considera todavía lejos de sus objetivos. Una Agenda Digital 2020 es la hoja de ruta para seguir mejorando.

X-Road y E-ID

La columna vertebral de la sociedad digital de Estonia es la plataforma descentralizada X-Road, a la cual están conectadas unas 1.000 instituciones. X-Road permite el intercambio seguro de datos entre bases de datos autorizadas, y se utiliza el principio de blockchain también para el almacenamiento. Es decir, a veces se usan sistemas de bases de datos en los que la administración de los datos está descentralizada. Los conjuntos de datos están vinculados entre sí por métodos criptográficos.

Además, todos los estonios tienen una tarjeta de identidad electrónica que se puede utilizar con un lector y una autenticación de dos factores, para la legitimación segura por internet, y que puede usarse para todos los servicios electrónicos. También permite hacer «firmas» electrónicas. Más del 90 por ciento de la población usa la tarjeta para servicios estatales a través de la plataforma E-Estonia, pero también para los servicios bancarios.

Fisuras y ataques

Pero todo esto también conlleva riesgos. Pronto se dieron a conocer brechas de seguridad en la tarjeta de identidad electrónica, en otoño de 2017. Los hackers pudieron acceder a los datos de alrededor de 750.000 personas, según informes de los medios. Sin embargo, según los expertos, se asignó a este problema la máxima prioridad. Incluso el Primer Ministro hizo declaraciones de inmediato al respecto. Y en poco tiempo se dispuso de una solución técnica con la cual se cerraron las fisuras.

Hace más de diez años, Estonia ocupó los titulares con una consecuencia negativa de la digitalización. En aquel momento, los hackers bloquearon repetidamente diferentes sitios de internet durante semanas, incluida la plataforma de internet del Estado y los sitios web de diferentes bancos.

Por eso la seguridad electrónica se convirtió en parte de la Defensa Nacional relativamente temprano. Después del ataque de hace diez años, las autoridades introdujeron un nuevo sistema para proteger los datos. Además, hoy todos los estonios pueden ver si alguien accedió a sus datos y cuándo, lo que permitiría detectar rápidamente los ataques.

Sede de la NATO para la ciberdefensa

Estonia se convirtió – probablemente también debido al ataque en aquel momento – en pionera de la ciberdefensa. Inmediatamente después de ingresar en la NATO, propuso la creación del correspondiente centro de competencias. Desde 2008, el Cooperative Cyber Defence Centre of Excellence (CCDCOE) tiene su sede en Tallin. Es una especie de think tank para la ciberdefensa.

El documento clave de la institución es el «Manual de Tallin», una colección de textos legales sobre el tema. Algunos expertos lo consideran una posible base para la extensión de las leyes internacionales de la guerra en el campo de la guerra electrónica. Pero el CCDCOE también lleva a cabo ejercicios de defensa concretos, durante los cuales los especialistas de los ejércitos implicados – los países de la NATO y los estados neutrales – deben defenderse contra ciberataques masivos.

Incluso los más jóvenes se ocupan intensamente de las ayudas digitales



Y por último, pero no menos importante, el CCDCOE escribe informes sobre países individuales, incluida la propia Estonia. Según dicho informe, debido al alto nivel de digitalización y su correspondiente vulnerabilidad, el tema de la ciberseguridad goza allí de una mayor prioridad que en la mayoría del resto de países.

Estrategia de ciberseguridad

El país fue uno de los primeros en adoptar una estrategia de ciberseguridad en 2008 y la renovó en 2014, escriben los autores. Las medidas de esta estrategia son secretas por naturaleza. Tampoco es público cuánto gasta el ejército en ciberseguridad. Después de todo, existe el compromiso de que este tema goza de alta prioridad.

Con datos altamente confidenciales, son imprescindibles soluciones de seguridad de la información de alta seguridad.

Sin embargo, los objetivos son públicos. Los objetivos son, entre otras cosas, una mayor concienciación frente a los ciberataques y la mejora de las capacidades para enfrentarlos. También se sabe cómo está estructurada organizativamente la defensa cibernética. Estonia no recibió solo elogios en el informe del CCDCOE. Por ejemplo, se observó que el órgano supremo de ciberseguridad no estaba ejerciendo su función de

supervisión en algunas fases y que carecía del apoyo de la política.

Papel importante de los socios

No obstante esto, los expertos coinciden en general en que Estonia puede tomarse como modelo de digitalización. Entre otras cosas, se remiten a los procesos más eficientes y, por lo tanto, más económicos. Las estimaciones sugieren que este pequeño país ahorra alrededor del dos por ciento del producto interno bruto gracias a la adopción generalizada de la firma digital.

Según los expertos, los Estados que deseen emular a Estonia deben prestar atención también a los riesgos de dicha estrategia de digitalización. La protección de los datos debe hacerse de manera adecuada en todos los niveles. Con datos altamente confidenciales, que son fundamentales para la existencia del Estado, es imprescindible contar con soluciones de seguridad de la información de alta seguridad. Esto es aplicable sobre todo a los campos de la diplomacia y la comunicación dentro de las fuerzas de seguridad, pero también a las áreas de State Governance, Defence e Internal Security. El factor decisivo, según los expertos, es conseguir los socios adecuados, con los necesarios conocimientos y experiencia, ya en una etapa temprana.



Control de acceso seguro mediante un dispositivo de lectura

Un puesto de trabajo de alta seguridad como base para el trabajo eficiente de la policía

Las organizaciones policiales a menudo operan a nivel nacional. El intercambio de informaciones confidenciales debe estar garantizado en todo momento para poder conservar la capacidad operativa. Un trabajo policial eficiente requiere además que, independientemente de la ubicación y del momento, la información clasificada esté accesible en la core network. La confidencialidad, autenticidad e integridad de esta información nunca debe ponerse en peligro.

Las exigencias de las organizaciones policiales son diversas, y la relevancia de la información para su capacidad operativa es alta. Por ejemplo, cuando los policías llevan a cabo su trabajo diario y realizan controles, necesitan tener acceso a los datos guardados en un puesto central. Es decir, la información confidencial, como los datos personales, debe ser accesible rápidamente en cualquier momento y en cualquier lugar, poder editarse y transmitirse fácilmente con alta seguridad, mientras que, al mismo tiempo, debe ser posible acceder a la información pública.

Se demandan soluciones de seguridad de la información que aborden los nuevos escenarios de amenazas como objetivo principal de ataque y permitan trabajar dentro y fuera de la organización para operar en un entorno de alta seguridad.

Ambos Compartments pueden operarse simultáneamente. La más alta seguridad de la información está garantizada en todo momento gracias a su separación constante.

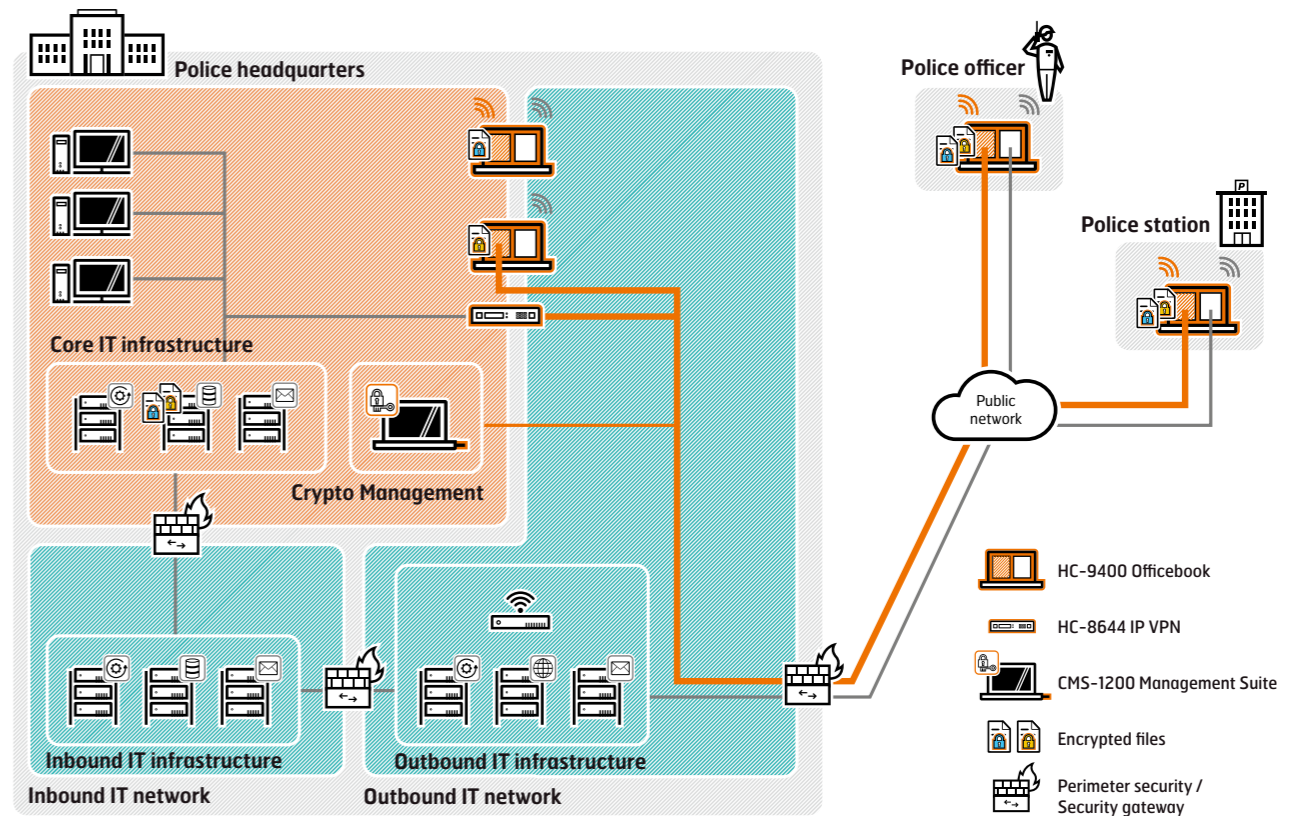
Por esta razón, las organizaciones policiales quieren una solución que permita trabajar sin afectar a la comodidad de uso y a la utilización de sistemas operativos comunes, como Windows, aplicaciones de Microsoft Office y navegadores web. Por medio de una gestión central de la seguridad, deben gestionarse también las relaciones de comunicación y los usuarios. Se requiere asimismo una infraestructura de gestión a medida para configurar y administrar el sistema.

La solución se llama cOffice Workplace

El sistema cOffice Workplace, basado en la tecnología Crypto SmartProtect, cumple plenamente estas exigencias y permite siempre un trabajo cómodo y con alta seguridad en el entorno de usuario conocido, tanto dentro como fuera de la organización. Esto significa que la comunicación con alta seguridad, con puestos exteriores interconectados en una red integral en todo el país, funciona permanentemente.

El HC-9400 Officebook es un componente central del sistema cOffice Workplace, adecuado para el uso estacionario y móvil. Tiene dos Compartments que proporcionan dos entornos de usuario completamente independientes. Con el primer Compartment se puede acceder a la información y aplicaciones centrales de la organización, que permiten el acceso seguro a la infraestructura informática de la central de la policía por medio de la solución de cifrado de alto rendimiento HC-8644 IP VPN. En el segundo Compartment, el usuario puede acceder a información públicamente disponible a través de un navegador web. Ambos Compartments pueden operarse simultáneamente. La más alta seguridad de la información está garantizada en todo momento gracias a su separación constante. La configuración y la administración de todo el sistema están garantizadas con la CMS-1200 Management Suite y la pasarela HC-8644 IP VPN.

Crypto International AG y Crypto Schweiz AG ofrecen una protección sin compromisos contra los ciberataques con cOffice Workplace.



cOffice Workplace permite un trabajo seguro y cómodo en un entorno de usuario seguro, dentro y fuera de la organización

Protección sin compromisos contra los ciberataques

aislados el uno del otro. Las informaciones confidenciales internas no corren peligro, incluso cuando se accede al mismo tiempo a una red pública (public network).

La más alta seguridad

Sobre la base de la tecnología Crypto SmartProtect, cOffice Workplace protege la información confidencial de la mejor manera posible contra el acceso de terceros, sin afectar al proceso de trabajo.

Máxima comodidad de uso

Los usuarios pueden trabajar en su entorno de usuario conocido, en cualquier lugar donde se encuentren. Además, es posible la sencilla conmutación entre los Compartments sin poner en peligro la información confidencial.

Alta eficiencia y flexibilidad

Para trabajar de manera eficiente y flexible pueden operarse simultáneamente dos entornos de usuario completamente

Integración simple

La integración en el entorno informático no requiere ninguna modificación fundamental de la infraestructura.



Crypto International AG
Zugerstrasse 42
6312 Steinhausen
Suiza

Crypto Schweiz AG
Zugerstrasse 42
6312 Steinhausen
Suiza

T +41 41 749 77 22
F +41 41 741 22 72
crypto@crypto.ch
www.crypto.ch

Crypto cSeminars

cSeminar Information Security Specialists
10 – 14 de septiembre de 2018

cSeminar Contemporary Cryptography
17 – 21 de septiembre de 2018

Los seminarios tienen lugar en la Crypto Academy
de Steinhausen.

Contacto e información detallada en
www.crypto.ch/seminars