CRYPTO

CRYPTO MAGAZINE

Nº 1 | 2017

Crypto SmartProtect – Cyberdefence auf höchstem Niveau

Geschätzte Leserin, geschätzter Leser

Die digitale Transformation und die damit einhergehende Vernetzung über öffentliche Netzwerke sind in vollem Gange, weshalb weltweit auch die Bedrohungen aus dem Cyberspace zunehmen. Nicht nur Unternehmen, auch Behörden und Organisationen sind davon betroffen. Vielfach haben es die Angreifer auf die Endgeräte der Mitarbeitenden abgesehen. So kann massgeschneiderte Malware beispielsweise in ein Ministerium eingeschleust werden, Daten abziehen und grossen Schaden anrichten. Um vor diesen hochprofessionellen Cyberattacken geschützt zu sein, braucht es mehrstufige Sicherheitselemente zum Schutz der primären Angriffsziele, den Computing-Plattformen. Die einzigartige von der Crypto AG entwickelte hochsichere Computing-Technologie Crypto SmartProtect eliminiert dieses Sicherheitsrisiko, schützt zuverlässig vor Cyberattacken und ermöglicht gleichzeitig gewohnt komfortables Arbeiten in der vertrauten Benutzerumgebung.

Mehr zur neuen Technologie, zu wichtigen Handlungsfeldern punkto Cyberdefence und möglichen Schutzkonzepten finden Sie in dieser Ausgabe des CryptoMagazine.

Giuliano Otth

President and
Chief Executive Officer

Impressum

Erscheint 2-mal jährlich | **Auflage** | 4'200 (Deutsch, Englisch, Französisch, Spanisch, Russisch, Arabisch)

Herausgeber | Crypto AG, Postfach 460, 6301 Zug, Schweiz, www.crypto.ch

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

Nachdruck | Honorarfrei mit Zustimmung der Redaktion, Belegexemplare erbeten, Copyright Crypto AG

Bildnachweis | Crypto AG: Titelseite, S. 2, 14, 21, 22 | Keystone: S. 18 | Prof. Dr. Bernhard M. Hämmerli: S. 7 | Shutterstock: S. 3, 8, 9, 10, 13, 20

Attacken aus dem Cyberspace

Betreiber von IT-Systemen müssen sich gegen eine wachsende Vielfalt von Attacken aus dem Cyberspace wappnen – das gilt auch für Organisationen mit hochprofessionellen Abwehrsystemen. Denn je grösser die Anzahl vernetzter Geräte und je komplexer die Strukturen sind, desto schwieriger ist es, gegen Gefahren wirksam geschützt zu sein. Neben Einfallstoren auf der technischen Seite gilt es auch zu verhindern, dass Mitarbeitende zum Risikofaktor werden.

Die zunehmende Vernetzung, Automatisierung, Digitalisierung sowie digitale Transformation lassen den Cyberspace rasant wachsen – den virtuellen Raum also, der alle global via Internet oder ähnliche Netzwerke verbundenen IT-Systeme umfasst. Damit nehmen auch die Angriffsflächen für Informationen, Anwendungen, Prozesse und die Kommunikation zwischen all diesen Systemen laufend zu.

In der Cyberdefence wird deshalb um die Informationssicherheit gerungen, also die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit digitaler Daten und datenverarbeitender Systeme. Insbesondere sind Behörden, Organisationen und Unternehmen darum bemüht, Datenabflüsse zu verhindern. Doch die Innovationsfrequenz ist sowohl auf der Seite der Angegriffenen, die sich laufend gegen neue Attacken schützen müssen, wie auch jener der Angreifer hoch.

Mannigfaltige Attacken

Bei den Formen der Attacken aus dem Cyberspace lässt sich eine grosse Vielfalt feststellen. Grundsätzlich sind dabei alle Aspekte von Informationssicherheit betroffen. Attacken auf die Vertraulichkeit von Informationen finden beispielsweise durch Advanced Persistent Threats (APT) statt. Darunter versteht man gezielte Attacken auf Behörden oder Organisationen. Der Angreifer verschafft sich dabei dauerhaften Zugriff auf ein Opfernetzwerk und weitet diesen sukzessive aus. APT erfordern ausgezeichnetes technisches Know-how, einen hohen Ressourceneinsatz und sind in der Regel schwierig zu erkennen. Grundsätzlich werden Vorfälle, bei denen sich Unberechtigte Zugriff auf Daten verschaffen, als Datenabfluss oder Datenleck bezeichnet – das gilt sowohl für gravierende Fälle wie APT wie auch für weniger weitreichendes Eindringen in IT-Systeme.

Typische Attacken auf die Integrität und Authentizität von Daten, also zwei weitere Aspekte der Informationssicherheit, sind sogenannte Defacements. Dabei werden die Inhalte einer Webseite verändert und verfälscht, um Besucher des entstellten Internetangebots in die Irre zu leiten. Üblich ist diese Taktik auch bei Versuchen, mittels Phishing an Passwörter zu gelangen. Angreifer versuchen hierbei, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Nutzers zu gelangen und damit Identitätsdiebstahl zu begehen. Der Begriff ist abgeleitet von «password» und «fishing», also «nach Passwörtern angeln».

Alle Aspekte der Informationssicherheit betroffen

Die Verfügbarkeit von Daten wird verhindert, indem etwa mittels Denial-of-Service (DoS)-Attacken dafür gesorgt wird, dass einzelne Dienste, Webseiten oder ganze Netze für Nutzer nicht mehr erreichbar sind. Wird eine DoS-Attacke durch mehrere Systeme gleichzeitig vollzogen, spricht man von verteilten DoS- oder DDoS-Attacken (Distributed Denial of Service). Bezeichnend für DDoS-Attacken ist die grosse Zahl der zum Einsatz kommenden Computer und Server – in der Regel werden Botnetze eingesetzt. Ein Botnetz ist ein Verbund von Rechnern, die allesamt von einem Schadprogramm befallen sind. Dieses macht sie zu sogenannten Bots – abgeleitet von «Roboter». Die betroffenen Rechner werden vom Botnetz-Betreiber mittels eines Command-and-Control-Servers kontrolliert und gesteuert. Eine weitere Methode, die Verfügbarkeit von Daten zu behindern, ist der Einsatz von Ransomware – also unbemerkt installierter, schädlicher Software. Diese schränkt die Verfügbarkeit von Daten so lange ein, bis der Besitzer eines Systems ein Lösegeld bezahlt oder eine andere Forderung des Angreifers erfüllt.

Arbeitsplätze im Visier der Angreifer

Stark zugenommen haben Attacken auf Endgeräte. Diese werden teilweise als «Sprungbrett» genutzt, um in weitere Ebenen eines IT-Systems einzudringen. Es ist deshalb zentral, dass Behörden und Organisationen hohe Standards für die Arbeitsplatzsicherheit einhalten. Das gilt grundsätzlich standortunabhängig, vermehrt in besonderem Masse aber insbesondere für Mitarbeitende, die ausserhalb der gewohnten Arbeitsumgebung tätig sind, etwa auf Reisen oder zu Hause. Gerade Mitarbeitende, die jederzeit erreichbar sein müssen, brauchen eine besonders sichere Infrastruktur. Dabei gilt es zu beachten, dass die erforderlichen Sicherheitsabläufe so komfortabel wie möglich ausgestaltet werden, damit Mitarbeitende nicht in Versuchung kommen, aus Gründen der Praktikabilität Sicherheitsstandards zu missachten.

Umgekehrt bietet die Nutzung von privaten Anwendungen am Arbeitsplatz – etwa jene von Social Media – ein Einfallstor für Attacken. Mittels Social Engineering werden Opfer dazu verleitet, eigenständig Daten preiszugeben, Schutzmassnahmen zu umgehen oder Schadprogramme zu installieren. Die Täter nutzen dabei menschliche Schwächen wie Neugier oder Angst, um die Opfer zu manipulieren. Diese klicken in der Folge beispielsweise auf Links, die unbemerkt Schadsoftware installieren, oder geben sensible Informationen wie Passwörter bekannt.

Kriminalität im Cyberspace

Die Grenzenlosigkeit des digitalen Raums hat zur Folge, dass die Identifikation von Angreifern oft schwierig, nicht selten kaum möglich ist. Dennoch lassen sich sowohl auf der Seite der Opfer als auch auf jener der Angreifer verschiedene Typen ausmachen. Die jüngsten, hochprofessionell durchgeführten Attacken zeigen: Hinter den Attacken stecken vielfach systematisch agierende Gruppierungen, die politische, wirtschaftliche oder staatsfeindliche Ziele verfolgen.

> Bei Attacken aus dem Cyberspace sind alle Aspekte von Informationssicherheit betroffen.

Geht es in erster Linie um Attacken, die der Bereicherung dienen oder ökonomischen Schaden anrichten sollen, spricht man von Cyberkriminalität. Auch Verbrechen wie etwa Identitätsdiebstähle oder Wirtschaftsspionage fallen in der Regel in diese Fallgruppe.

Der Cyberspace ist aber auch ein Gebiet, in dem Krieg geführt wird. Es ist unbestritten, dass Kriegsführung im Informationszeitalter immer auch digitale Komponenten beinhaltet. Mitte 2016 hat die NATO den virtuellen Raum offiziell zum Kriegsgebiet erklärt. Das bedeutet: Dort ausgeführte Attacken können entsprechende Folgen auslösen wie Attacken auf dem Boden, aus der Luft oder im Wasser.

Das Schadensausmass eines Cyberwar ist denn auch enorm. Die mit informationstechnischen Mitteln im virtuellen Raum geführte kriegerische Auseinandersetzung wird oft in drei Formen kategorisiert: Zielt ein Angreifer darauf ab, die gegnerischen Netzkapazitäten lahmzulegen oder zu zerstören, wird von Computer Network Attacks (CNA) gesprochen. Computer Network Exploitation (CNE) umfasst Handlungen, deren Ziel es ist, im nachrichtendienstlichen Sinne Informationen auf gegnerischen Rechnern zu ermitteln. Die zum Schutz der eigenen Computer und Computersysteme eingesetzten Massnahmen werden als Computer Network Defense (CND) bezeichnet.

In der Praxis allerdings ist die Abgrenzung von Cyberwar und Cybercrime oft schwierig. Zum einen ist die Identifikation der Angreifer häufig nicht möglich, zum anderen können auch Attacken auf private Unternehmen kriegerische Ziele verfolgen. Darunter ist etwa die Behinderung des gesellschaftlichen und wirtschaftlichen Alltags eines Landes zu verstehen. Diese Ziele können beispielsweise durch Attacken auf private Unternehmen verfolgt werden, die für die Bereitstellung kritischer Infrastruktur wie etwa der Stromversorgung verantwortlich sind.

Rasante Entwicklungen erwartet

Zwei Entwicklungen beschleunigen die Spirale von Attacken und Gegenmassnahmen: einerseits die Zunahme von elektronischen Geräten und deren Vernetzung, andererseits die wachsende Komplexität von Aufgaben, die diese übernehmen können. Ein Blick auf Trends wie Industrie 4.0 – also die prozessintegrierte Zusammenarbeit über Unternehmens- und Organisationsgrenzen hinweg, die eine Vernetzung in vollkommen neuen Dimensionen bedingt – zeigt klar, dass sich nicht nur eine Fülle von Möglichkeiten eröffnet, sondern auch neue Angriffsflächen geschaffen werden.

Umso wichtiger ist es, dass man bei der Ausarbeitung von wirksamen Schutzmechanismen neben den Massnahmen, die auf den Schutz der Daten während ihrer Übertragung zielen, auch die wachsende Zahl der Endgeräte im Blick behält. Nicht zuletzt sollen auch privat genutzte Geräte in die Sicherheitsüberlegungen miteinbezogen werden – damit auch die kleinsten Schlupflöcher gestopft werden können, bevor sich Angreifer über sie Zugang zu ganzen Systemen verschaffen.

INTERVIEW

«Erfolgversprechend ist, wenn Organisationen diverse Strategien gleichzeitig verfolgen»

Attacken aus dem Cyberspace haben massiv zugenommen, auf Seiten der Angreifer ist ein enormer Professionalisierungsschub zu beobachten. Bernhard Hämmerli, Professor der Informatik an der Hochschule Luzern, nimmt im Gespräch eine Einordnung der Angriffe und ihrer Urheber vor und beleuchtet Wege, wie Behörden und Organisationen sich effizient schützen können.

Die Cyberrisiken haben in den letzten Jahren markant zugenommen. Wie beurteilen Sie den Status quo der Cybersicherheitslage für Unternehmen und Behörden?
Werden die Schätzungen des Weltwirtschaftsforums für Cybercrime im Jahr 2015 auf die Schweiz umgerechnet, resultieren rund 5 Milliarden US-Dollar für die Schweiz – das entspricht einer Vervierfachung seit 2013. Die Ausgaben für nationale Vorkehrungen sollen in der Schweiz hingegen nur rund 70 Millionen betragen. Die Entwicklung der geschätzten Schäden aus Cybervorfällen zeigt einerseits ein dramatisches Wachstum auf, andererseits besteht aus meiner Sicht eine Diskrepanz zwischen den geschätzten Verlusten und den Investitionen, die in Gegenmassnahmen getätigt werden.

Worauf ist diese Entwicklung zurückzuführen?
Auf der Seite der Angreifer hat in den vergangenen Jahren eine enorme Professionalisierung eingesetzt. Es geht nicht mehr wie zur Zeit der ersten Hacker um Anerkennung, sondern um handfeste finanzielle Gewinne. Und um Dominanz im Cyberspace – gerade wenn wir von staatlichem Handeln in dem Bereich sprechen.

Wie ist ein effektiver Schutz vor Cyberrisiken aufgebaut?
Bis vor etwa zehn Jahren sind viele Organisationen davon ausgegangen, dass Investitionen in Schutzmassnahmen genügen, um Schäden durch Angriffe zu verhindern. Das hatte lange seine Richtigkeit. Doch die Attacken haben massiv zugenommen, inzwischen ist es so, dass Behörden und grosse Organisationen nahezu ständig angegriffen werden. Und diese Attacken bringen erhebliche Risiken für die Informationssicherheit mit sich – sie gefährden also die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit digitaler Daten.

Wie gilt es darauf zu reagieren?
Es gibt zwei grundsätzliche Strategien: Einerseits kann man auf Policy-Ebene auf Abschreckung setzen, etwa durch strenge Strafen. Andererseits muss man als Organisation bereit sein, wenn etwas passiert. Letzteres wird unter den Schlagworten «detection and response» zusammengefasst, Angriffe sollen also zeitnah entdeckt und Gegenmassnahmen rasch eingeleitet werden. Zudem muss die Sicherheitsarchitektur so angelegt sein, dass eine Attacke auf einen Arbeitsplatz nicht gleich das gesamte IT-System verletzlich macht.

Können Sie Aussagen über die Urheber der Angriffe und deren Motive machen?
Zum einen sind es finanzielle Motive, zum anderen werden mit Attacken aus dem Cyberspace politische Ziele verfolgt. Nicht selten gibt es auch ein Motivgemenge aus finanziellen und politischen Zielen.

Können Sie eine Typologie der häufigsten Opfer vornehmen, auch mit Blick auf die Unterscheidung von Cyberwar und Cybercrime?
Hier zu unterscheiden ist schwierig, da es nicht selten Vermischungen gibt. Auf der Seite der Opfer lassen sich alle denkbaren Akteure finden: von der Privatperson, die einem Phishing-Mail auf den Leim geht, über Firmen, deren Betriebsgeheimnisse ausspioniert werden, bis hin zu Staaten, die sich im Cyberspace gegenseitig beobachten, um ihr Handeln auf so erlangte Informationen stützen zu können.

Welche Formen von Attacken auf Behörden und Unternehmen sind üblich?
Es gibt eine ganze Palette von Attacken. Oft geht es darum, Nutzer dazu zu verführen, dass sie etwas anklicken – sei es ein Link oder ein Attachment, das per E-Mail verschickt wurde. So wird Malware installiert, über die dann beispielsweise Daten abgesaugt werden. Oft dient solche Malware auch als erstes Sprungbrett, um in das IT-System einer gesamten Organisation einzudringen. Neben der Überwachung kann aber auch das Beeinträchtigen der Funktionalität ein Ziel von Attacken sein.

Welche Formen von Attacken sind besonders verheerend und warum?
Das kann man pauschal nicht sagen, es kommt auf die Tätigkeit einer Organisation sowie die Ziele einer Attacke an. Unbestritten ist allerdings, dass ein über längere Zeit unentdecktes Eindringen in ein IT-System extrem problematisch sein kann. Einerseits können so die Tätigkeiten einer Organisation über längere Zeit überwacht werden, andererseits haben Angreifer die Möglichkeit, den optimalen Zeitpunkt für ihr Ziel abzuwarten. Auch deshalb ist ein «detection and response»-Team zentral. Es sind Fälle bekannt, in denen Angreifer über Jahre Zugriff auf kritische IT-Systeme hatten.

Wie können staatliche Behörden sich selber und nationale Unternehmen schützen?
Es braucht Lagezentren, die ununterbrochen Aktivitäten im Cyberspace überwachen und über Gefahren informieren: Dieser Bereich sollte in der Schweiz verstärkt werden. Mit der Melde- und Analysestelle Informationssicherung, kurz MELANI, haben wir in der Schweiz bereits ein Zentrum mit primärem Fokus auf die Meldung von Vorfällen und die anschliessende Analyse. Zudem sollte die internationale Zusammenarbeit bezüglich Austauschs von Bedrohungen und Verletzlichkeiten weiter verstärkt werden.

Wie gross ist das Risiko, das vom «Faktor Mensch» ausgeht? Studien zeigen, dass über 50 Prozent der primären Einfallstore auf Fehlverhalten von Mitarbeitenden zurückzuführen ist.
Die Erstinfektion eines IT-Systems gelingt tatsächlich sehr oft durch das Ausnutzen von menschlichem Fehlverhalten. Gehen wir von einer Behörde mit 10'000 Mitarbeitenden aus, die alle von einem Angreifer innerhalb eines Jahres 100 E-Mails erhalten,

Prof. Dr. Bernhard M. Hämmerli unterrichtet seit 1992 an der Hochschule Luzern und seit 2009 zudem an der Norwegian University of Science and Technology Informatik. Sein Fokus in Lehre und Forschung liegt auf den Gebieten Kommunikation, Netzwerke und Informationssicherheit. Er ist Spezialist für den Schutz von kritischen Infrastrukturen. Seit 2012 leitet er die Plattform ICT Security der Schweizerischen Akademie der Technischen Wissenschaften.

über die das Herunterladen von Malware initiiert werden soll. Das ergibt 1 Million Angriffe, die mit relativ wenig Aufwand getätigt werden können. Wenn nur ein Mitarbeitender ein einziges Mal auf den Link klickt, hat der Angreifer sein Ziel erreicht. Die Wahrscheinlichkeit, dass in einem von einer Million Fällen ein Fehler passiert, ist nun einmal ziemlich hoch.

Wie kann man den «Faktor Mensch» am besten im Griff behalten?
Erfolgversprechend ist in der Regel, wenn Organisationen diverse Strategien gleichzeitig verfolgen. Zum einen gilt es, auf der technischen Seite innerhalb des IT-Systems weitgehend in sich geschlossene Räume zu bilden, so dass der Schaden, der durch das Eindringen in ein IT-System erfolgt, klar begrenzt bleibt. Es empfiehlt sich auch, wann immer möglich Tätigkeiten zu virtualisieren. Schliesslich ist es zentral, die Mitarbeitenden kontinuierlich mit Blick auf das Bewusstsein, die Attitüde und das Verhalten zu sensibilisieren.

> Cyberattacken bringen erhebliche Risiken für die Informationssicherheit mit sich – sie gefährden die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit digitaler Daten.

Bei massgeschneiderten Angriffen auf Endgeräte versagen oft bestehende Sicherheitskonzepte. Wie kann die Informationssicherheit auf Endgeräten gewährleistet werden?
Die Problematik besteht aus mehreren Komponenten: Pro Benutzer ist nicht mehr nur ein Gerät, sondern oft zwei bis fünf Endgeräte im Einsatz. Mit Mobile-Device-Management (zentralisierte Verwaltung) und Virtual Desktop (Virtualisierung des PC-Desktops im Rechenzentrum) kann die Sicherheitssituation im Unternehmen massiv verbessert werden. Weiter geht es auch hier um die Mitarbeitenden. Hier hilft, wie bereits erwähnt, die stetige Verhaltensschulung. Trotzdem ist davon auszugehen, dass auch damit keine hundertprozentige Sicherheit erlangt wird. Um ein höheres Schutzniveau zu erreichen, müssen alle Aspekte einer Sicherheitsarchitektur berücksichtigt werden, damit die Vertraulichkeit der Informationen jederzeit gewährleistet ist.

Bei hoher Informationssicherheit ist häufig der Bedienkomfort eingeschränkt. Müssen IT-Sicherheitsverantwortliche mit diesem Kompromiss leben?
In der Vergangenheit war es tatsächlich so, dass praktisch alle IT-Sicherheitsmassnahmen nachträglich eingebaut wurden und es für die Anwender oft sehr unangenehm war, sie zu befolgen. Der Bedienbarkeit, der sogenannten Usability, wird heutzutage sehr viel mehr Aufmerksamkeit geschenkt und gegenwärtig sind Produkte auf dem Markt, die Sicherheitsfunktionen praktisch ohne Einschränkung des Bedienkomforts integrieren.

Wo sehen Sie künftig die wichtigsten Handlungsfelder punkto Cyberdefence?
Es gibt viele Ansatzpunkte, ich möchte nur kurz ein Beispiel ausführen. Zentral scheint mir, dass auf nationaler Ebene die forensischen Kompetenzen ausgebaut werden. Attacken sollten also vor Ort effizienter und effektiver untersucht werden können. Gerade kleinere Staaten wie die Schweiz müssen regelmässig auf private Anbieter von forensischen Diensten – teilweise auch aus dem Ausland zurückgreifen –, auch wenn Fragen der nationalen Sicherheit betroffen sind. Bei den Unternehmen und Organisationen scheint es mir wichtig, dass ein ganzheitlicher Ansatz, der die verschiedenen Dimensionen der Informationssicherheit berücksichtigt, gefahren wird. Die Benutzer sollen in ihrem Bedienkomfort trotz hoher Informationssicherheit nicht eingeschränkt werden, sondern möglichst in ihrer gewohnten Benutzerumgebung effizient, komfortabel und hochsicher arbeiten können.

Crypto cSeminars

Die Crypto AG richtet sich mit den Crypto cSeminars an Fachpersonen, die mit der Informationssicherheit von Unternehmen und Organisationen betraut sind. Profundes Fachwissen über Informationssicherheit, Cyberkriminalität und Kryptografie wird von erfahrenen Spezialisten vermittelt. Im Zeitalter der Digitalisierung ist solides Fachwissen über Cyberdefence entscheidend. Teilnehmer der Crypto cSeminars werden mit diesem Know-how ausgestattet und können damit für den umfassenden Schutz sensibler Informationen und der ICT-Infrastruktur im Unternehmen sorgen.

Die Crypto cSeminars werden an der Crypto Academy in Steinhausen / Zug, Schweiz, durchgeführt. Weitere Informationen sind unter **www.crypto.ch/seminars** abrufbar.

Der Feind im System

Auch Organisationen mit hohem Bewusstsein für IT-Sicherheit sind vor Cyberattacken nicht gefeit. Immer wieder wurden Attacken publik, die bei Experten wie auch in der Öffentlichkeit für Verwunderung sorgten. Denn vermeintlich hochsichere Behörden oder Unternehmen wurden Opfer von Angreifern, welche gezielt die Endgeräte von Mitarbeitenden angriffen. Für die IT-Sicherheitsarchitektur gilt es deshalb mehr denn je, das Augenmerk auf die Endgeräte der Mitarbeitenden zu legen und diese konsequenter von öffentlichen Netzen zu trennen.

Damit hatte niemand gerechnet. Die Behörde wähnte sich in Sicherheit. Man war überzeugt, umfassend vor jeglicher Art von Cyberattacken geschützt zu sein. Umso grösser war der Schrecken, als die IT-Sicherheitsverantwortlichen feststellen mussten, dass Cyberkriminelle über Monate oder vielleicht sogar Jahre in ihrem vermeintlich sicheren IT-System nach Belieben ein- und ausgingen. Zurück blieben vor allem viele Fragezeichen. Im Nachhinein war es nicht mehr möglich, alle Einzelheiten des Angriffs zu rekonstruieren. Welche Informationen und Daten weggekommen sind, wie sich die Angreifer Zugang zu den internen Netzen verschafft haben, welche Systeme infiziert wurden – darüber kann nur spekuliert werden.

Es wurde ein vom Staat in Auftrag gegebener Untersuchungsbericht erstellt und veröffentlicht – mit dem Ziel, dass sich andere Behörden und Unternehmen gegen solche Angriffe besser wappnen können. Wer die Täter sind, ist allerdings bis jetzt unbekannt.

Mit bekannter Software unerkannt im internen Netz
Die Cyberkriminellen in diesem Fall gingen äusserst vorsichtig vor. Daher ist nicht gesichert, ab wann sie überhaupt tätig waren. Gewiss ist, dass sie eine seit Jahren bekannte Malware benutzten – bestehend aus verschiedenen Trojanern. Die gute Tarnung im System ist ein Merkmal dieser Technologie. Sie benötigt beispielsweise keine Administratorenrechte, auf die viele klassische Antivirenprogramme anspringen.

Angreifer gehen äusserst vorsichtig vor und bewegen sich unbemerkt

Die Angreifer waren zudem äusserst geduldig. Sie griffen innerhalb der Behörde nur Opfer an, von denen sie sich etwas versprachen. Das fanden sie heraus, indem sie die Aktivitäten der einzelnen Mitarbeitenden am Computer über ihre eingeschleuste Malware genau beobachteten. Wahrscheinlich holten die Täter ausserdem weitere Informationen über den Status der beobachteten Personen in der Organisation ein – zum Beispiel auch solche, die auf Social-Media-Netzwerken frei zugänglich sind.

Das Hauptangriffsziel war zunächst der Verzeichnisdienst des IT-Systems, das sogenannte Active Directory. Dieses ist das zentrale Adressbuch und von da aus kann auf weitere Anwendungen und Geräte zugegriffen werden. Auch beim eigentlichen Diebstahl waren die Angreifer vorsichtig. Um keine Anomalien im Netzverkehr zu verursachen, gab es während des Angriffs Zeiten mit grosser, aber auch solche mit geringer Aktivität.

Technisch kamen beim Angriff sogenannte Command-and-Control-Server zum Einsatz. Über diese wurden sogenannte Wasserlöcher (Waterholes) aktiviert. Das sind von den Hackern manipulierte Internetseiten, welche die Opfer regelmässig besuchen und denen sie daher auch vertrauen. Laut dem Bericht wurden von diesen Servern – es waren viele im Einsatz – Aufträge an die infizierten Geräte gesendet. Es soll sich um ein ausgeklügeltes System mit vielen nicht lokalisierbaren Servern gehandelt haben, was ebenfalls lange Zeit verhinderte, dass die Attacke bemerkt werden konnte.

Professioneller Datendiebstahl
Laut dem Untersuchungsbericht war der Angriff auf die Behörde beispielhaft. Experten unterscheiden bei Hackerangriffen im grossen Stil grob folgende Phasen: die Opferevaluation, die Erstinfektion, die Infektion und die eigentliche Exfiltration.

In der Evaluationsphase geht es darum, möglichst viele Informationen über das Angriffsziel zu sammeln. Dazu gehören auch eine Sammlung von IP-Adressen und Schemata, wie sich die möglichen Opfer im IT-System bewegen. Solche Informationen können zunächst passiv, später aber zusätzlich auch aktiv gesammelt werden. Vor dem eigentlichen Angriff müssen auch die Wasserlöcher eingerichtet, also die von den Opfern häufig benutzten Internetseiten manipuliert werden. Alternativ können auch Mails vorbereitet werden, über die der Angriff erfolgen soll.

Die Erstinfektionsphase ist dann durch das Aktivieren der Wasserlöcher oder der manipulierten Mails gekennzeichnet. Der eigentliche Angriff beginnt. Gelingt er, wird das Verhalten des Opfers genau untersucht – und auf dieser Basis ein geeignetes Angriffstool ausgewählt. Man spricht dabei von sozialmanipulativen Attacken.

In der eigentlichen Infektion bewegt sich der Täter über verschiedene Angriffstools im Netzwerk. Oft wird dafür ein erstes Aufklärungstool mit bescheidenen Fähigkeiten installiert. Dieses wird später durch eine umfassendere Malware abgelöst, welche sich im System festsetzt. Mit dieser kann sich der Angreifer dann seitwärts im System fortbewegen und nach Informationen suchen. Typisch für diese Seitwärtsbewegung ist, dass der Angreifer mit der Zeit zusätzliche Berechtigungen und Privilegien erhält – indem er beispielsweise Passwörter ausspioniert. Um nicht von Überwachungstools entdeckt zu werden, werden die Datenströme oft nicht direkt gesendet, sondern indirekt. Beim eigentlichen Diebstahl werden die Daten oft komprimiert und fragmentiert und zum Teil chiffriert versandt– damit der Angriff auch in dieser entscheidenden Phase nicht auffliegt.

> Das Ziel ist, den Angreifern das Leben so schwer wie möglich zu machen. Entscheidend ist, dass das eigene System dauernd und eng überwacht wird, um Spuren laufender Attacken sofort zu entdecken.

Durch Informationsaustausch IT-Sicherheit verstärken
Die Autoren des Untersuchungsberichts kamen zum Schluss, dass solche Attacken kaum verhindert werden können. Es müsse aber das Ziel sein, den Angreifern das Leben so schwer wie möglich zu machen. Entscheidend sei, dass das eigene System dauernd und eng überwacht werde, um Spuren laufender Attacken sofort zu entdecken. Wichtig sei ausserdem ein Informationsaustausch über erfolgte oder versuchte Infektionen.

Diese Einschätzung teilen auch die Experten der Crypto AG. So gilt eine effektive Systemüberwachung als essenzieller Bestandteil eines umfassenden Abwehrdispositivs. Eine solche biete die Chance «unlogische» Verbindungen oder sonstige Anomalien zu erkennen. Um maximale IT-Sicherheit gewährleisten zu können, bestünden dank erheblicher Fortschritte in der Informations- und Kommunikationstechnologie heute aber durchaus zusätzlich Möglichkeiten, IT-Systeme so zu bauen, dass sie vor Angriffen dieser Art umfassend geschützt seien.

Entscheidend sei dabei, dass innerhalb einer Organisation unterschiedliche Sicherheitsstufen zugeteilt werden und die Kommunikation ausschliesslich innerhalb dieser Zonen stattfinde. Klassifizierte Informationen der Stufe Top secret dürften zum Beispiel die High-security zone nie verlassen. Zugriff auf sie sollten zudem möglichst wenige Nutzer haben. Bei den nachrangigen Sicherheitszonen sind die vorhandenen Daten weniger sensibel und der Sicherheitsaspekt folglich weniger zentral; auch sie müssen jedoch abgeschlossen sein, damit die Sicherheit des Gesamtsystems nicht gefährdet ist.

Die High-security zone ist eine isolierte Zone und verfügt über keinen Zugang zum Internet. Von der Secure zone kann nur via Perimeterschutz der Zugriff aufs Netz sicher gewährleistet werden.

Im vorhin erwähnten Hackerangriff sei das Schlüsselproblem gewesen, dass zwar verschiedene Sicherheitszonen definiert worden seien, es zwischen diesen jedoch wahrscheinlich «Löcher» gegeben habe, meinen Fachleute. Diese Tatsache hätten die Angreifer ausgenutzt; nur dank diesen Lücken hätten sie sich seitwärts im System vorwärtsbewegen können – und seien so Schritt für Schritt den Firmengeheimnissen näher gekommen.

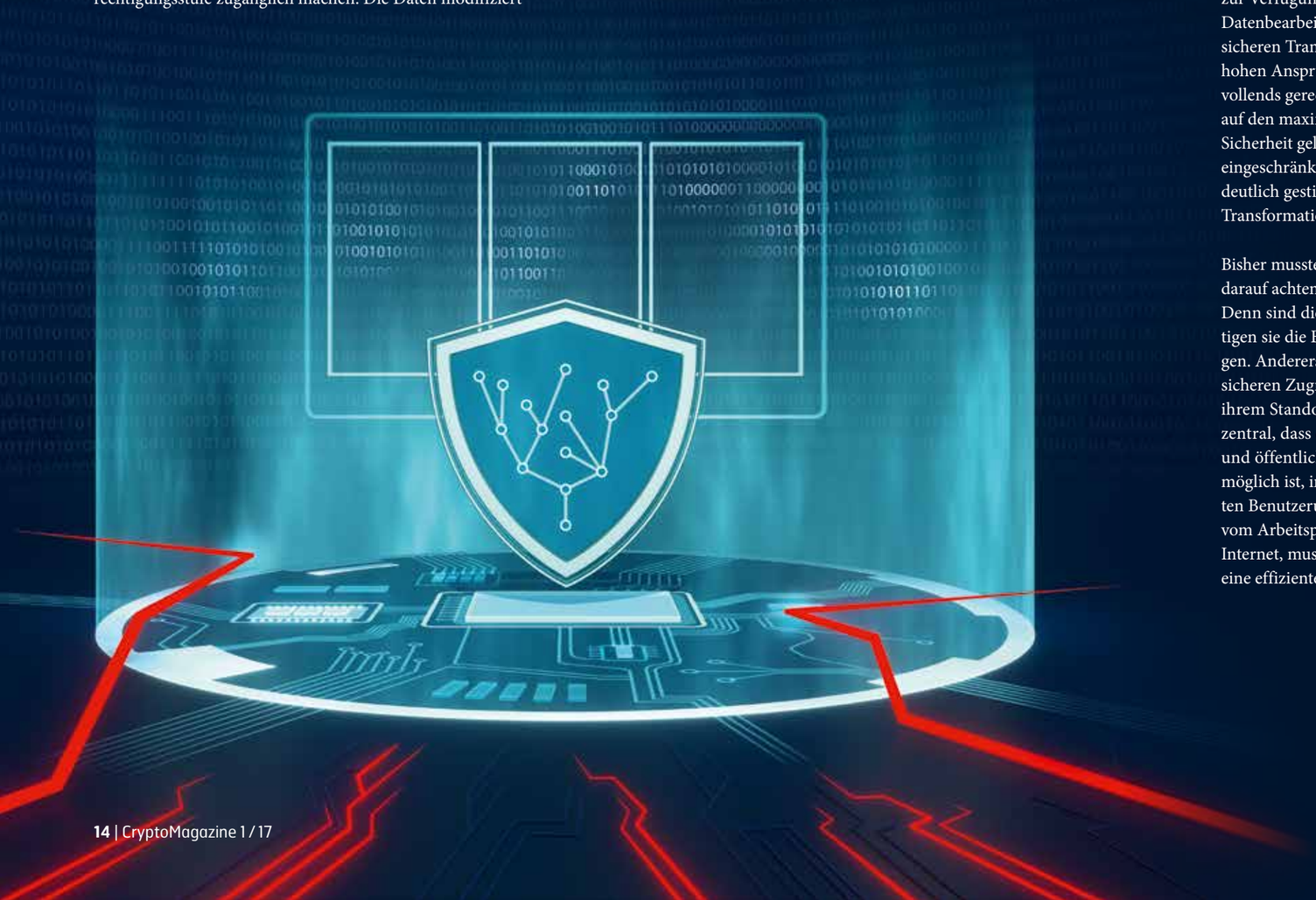
Technologisch ist es laut den Experten der Crypto AG seit geraumer Zeit kein Problem mehr, innerhalb der Sicherheitszonen eine hochsichere Kommunikation zu garantieren. Selbst wenn extern gearbeitet wird, zum Beispiel an einem Laptop, können Daten via geschützte VPN-Tunnels (Virtual Private Network) hochsicher transportiert werden. Dies erreicht man durch die direkte Integration hardwarebasierter Komponenten, mit denen sich eine Vielzahl sicherer VPN-Tunnels anlegen lassen, die mit voneinander unabhängigen Schlüsseln individuell chiffriert werden können. Bisher galt: Werden sensible Daten auf einem Endgerät bearbeitet, erfolgt dies nur mit minimalem Schutz und bietet Cyberkriminellen so ein leicht angreifbares Ziel.

Diese Sicherheitslücke zu schliessen ist der Crypto AG nun gelungen, indem Endgeräte mittels einer Kombination aus mehreren hard- und softwarebasierten Sicherheitselementen geschützt werden. Die neue Technologie Crypto SmartProtect bietet dafür den umfassendsten Schutz für sensible Informationen im zivilen wie auch militärischen Einsatzbereich. Mehr zu Crypto SmartProtect finden Sie im folgenden Artikel auf Seite 14.

Crypto SmartProtect für höchste Informationssicherheit und maximalen Bedienkomfort

«Komplexität ist der schlimmste Feind der Sicherheit», lautet ein Bonmot unter IT-Experten. Tatsächlich werden aber die IT-Systeme von Behörden, Organisationen und Unternehmen immer komplexer. IT-Sicherheitsverantwortliche geraten so vermehrt in ein Dilemma zwischen den Ansprüchen an die Informationssicherheit und jenen an die Benutzerfreundlichkeit. Crypto SmartProtect löst diesen scheinbaren Widerspruch auf.

Die situativen Umstände verlangen rasches Handeln: Der Mitarbeitende ist im Ausland unterwegs, als ihm das Hauptquartier klassifizierte Daten der Stufe Top secret auf seinen Rechner zustellt. Auszüge dieser klassifizierten Information muss er nun weiteren Personen mit der gleichen Berechtigungsstufe zugänglich machen. Die Daten modifiziert er und verschickt sie anschliessend über das Internet. Dabei gilt es, sowohl die restriktiven Sicherheitsvorschriften der Organisation zu befolgen wie auch sicherzustellen, dass die Vertraulichkeit, Integrität und Authentizität der sensiblen Informationen gewahrt bleiben.



Ein solches Szenario stellt nicht nur den Mitarbeitenden vor grosse Herausforderungen, sondern auch den IT-Sicherheitsverantwortlichen. Es liegt in seiner Verantwortung, dem Kader benutzerfreundliche, aber auch hochsichere IT-Infrastrukturen und Arbeitsplätze zur Verfügung zu stellen. Dieser Spagat zwischen Sicherheit und Benutzerfreundlichkeit erforderte bis vor kurzem Kompromisse. Nicht zuletzt verlangte das Szenario, getreu dem Grundsatz «Nur die physische Trennung garantiert maximale Informationssicherheit», nach mehreren Systemen.

Mit Crypto SmartProtect stellt die Crypto AG eine Technologie zur Verfügung, die alle Ansprüche an hochsichere, lokale Datenbearbeitung auf dem Endgerät einerseits und deren sicheren Transport andererseits erfüllt, sowie gleichzeitig den hohen Ansprüchen und Bedürfnissen der heutigen Arbeitswelt vollends gerecht wird. Bei der Entwicklung wurde der Fokus auf den maximalen Bedienkomfort einschliesslich maximaler Sicherheit gelegt, der nicht durch Sicherheitsanforderungen eingeschränkt wird, die wegen zunehmender Cyberattacken deutlich gestiegen sind und infolge des Trends zur digitalen Transformation weiter steigen werden.

Bisher musste der IT-Sicherheitsverantwortliche einerseits darauf achten, dem Benutzer nicht zu enge Fesseln anzulegen. Denn sind die technischen Restriktionen zu strikt, beeinträchtigen sie die Effizienz oder werden im Extremfall gar umgangen. Andererseits brauchen manche Mitarbeitende jederzeit sicheren Zugriff auf sensible Informationen, unabhängig von ihrem Standort und der benutzten Plattform. Dabei ist es zentral, dass der Umgang mit klassifizierten, unklassifizierten und öffentlichen Informationen gleichzeitig und komfortabel möglich ist, insbesondere auch unter Anwendung der gewohnten Benutzerumgebung. Kommt hinzu: Der direkte Zugang vom Arbeitsplatz zu externen Informationsquellen, etwa dem Internet, muss bereitgestellt werden, um den Mitarbeitenden eine effiziente und vertraute Arbeitsumgebung zu bieten.

> Crypto SmartProtect schützt zuverlässig vor Cyberattacken und ermöglicht sicheres und komfortables Arbeiten in vertrauter Umgebung.

Angriffsmuster verändern sich

In der Vergangenheit wurden in der Regel alle IT-Systeme einem einheitlichen Netz zugeordnet, an dessen Schnittstelle zum Internet eine zentrale Sicherheitsgateway-Lösung für die Informationssicherheit zuständig war. Diese Sicherheitsarchitektur erfüllt zwar den Anspruch an Einfachheit, bietet aber nur ungenügende Informationssicherheit (siehe Artikel auf Seite 10). Hatte ein Angreifer das Sicherheitsgateway überwunden, stand das gesamte Netz mit allen Komponenten offen. Deshalb wurden verschiedene Sicherheitszonen eingerichtet, die eine Zuteilung von Daten gemäss Klassifizierung erlaubten; beispielsweise dreistufige Modelle, die aus einer High-security zone, einer Secure zone und einer Trusted zone bestehen. Die Klassifizierung ist dazu da, um Informationen entsprechend ihrer Wichtigkeit oder Vertraulichkeit ablegen zu können.

Das Prinzip des Verbots zonenübergreifender Zugriffe sorgt dabei zusätzlich für Sicherheit. Es verhindert, dass Angreifer ein kompromittiertes System mit weniger starken Sicherheitsmassnahmen als «Sprungbrett» für das ganze Netz nutzen können. Wird ein IT-System kompromittiert, sind lediglich die IT-Systeme derselben Zone und Organisationseinheit in Gefahr. Diese Architektur bietet zwar einen hohen Informationsschutz, lässt den Zugang zu klassifizierten und unklassifizierten Informationen allerdings nur via separate Notebooks oder PCs zu, was die Anwenderfreundlichkeit nicht fördert und eher umständlich ist.

Technologiearchitektur für umfassenden Schutz gegen Cyberattacken

Nicht nur die Kompromisse zwischen Informationssicherheit und Bedienkomfort sind den IT-Verantwortlichen ein Dorn im Auge. Auch die laufend zunehmende Komplexität der Betriebssysteme und Applikationen handelsüblicher Betriebssysteme macht ihnen zu schaffen. Die auf Kompatibilität, Funktionalität und Performance ausgerichteten Systeme basieren auf Codes, die mehrere Millionen Zeilen umfassen. Selbstredend schlummern in derartigen Architekturen massive Sicherheitsrisiken. Moderne Betriebssysteme und Applikationen sind heute aus dem Arbeitsbereich nicht mehr wegzudenken. Damit diese Betriebsumgebungen sicher betrieben werden können, müssen sie in ein sicheres Compartment eingeschlossen werden, damit sie vor äusseren Angriffen wirkungsvoll geschützt sind. Dieser Schutz wird mittels des sicheren Betriebssystems Crypto SmartProtect OS erreicht. Das Sicherheits-Betriebssystem stellt vollständig isolierte Compartments bereit. Die Benutzerumgebungen in diesen Compartments werden durch das Sicherheits-Betriebssystem und unter Kontrolle des Microkernels – konsequent getrennt – auf dem gleichen Prozessor ausgeführt. Die Architektur des Sicherheits-Betriebssystem basiert auf dem Grundsatz von Security by Design. Alle Komponenten sind strukturiert, isoliert sowie unabhängig verifizierbar. Die Berechtigungen für die Verwendung von Services der einzelnen Komponenten sind unveränderbar verankert und der Microkernel setzt diese konsequent durch. Dadurch werden jegliche Angriffe auf das Crypto SmartProtect OS und somit auch auf die Benutzerumgebungen verhindert.

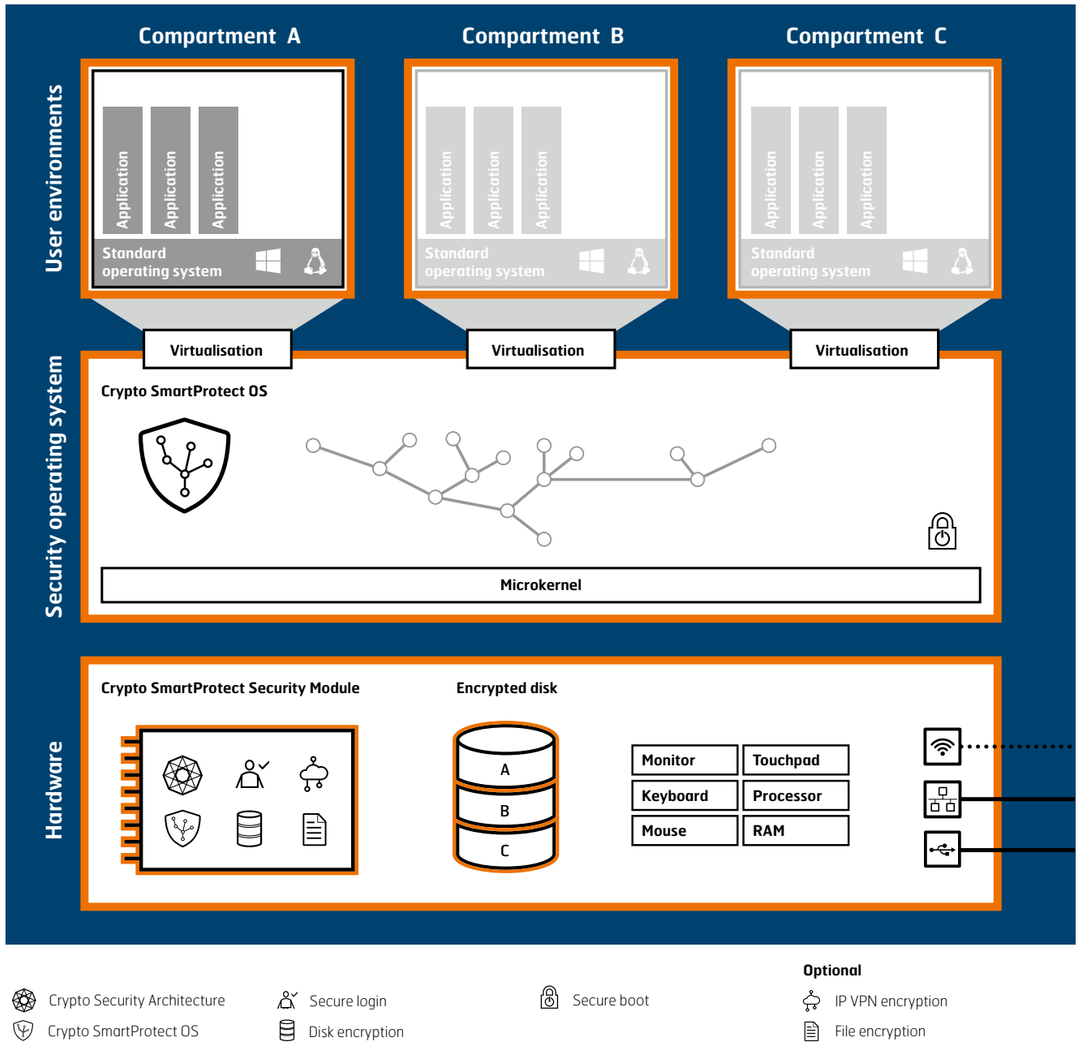
> Crypto SmartProtect ermöglicht dem Mitarbeitenden, Daten auf seinem Rechner gleichzeitig in unterschiedlichen Sicherheitszonen in konsequent getrennten Compartments zu erstellen, bearbeiten, speichern, löschen und übermitteln.

Für den Fall, dass auf demselben Endgerät ein Zugang zu unterschiedlichen Sicherheitszonen oder getrennten Netzwerken erforderlich ist, können mehrere voneinander isolierte und geschützte Compartments gleichzeitig betrieben werden. So kann in einem Compartment in einer geschlossenen, vertrauenswürdigen Benutzerumgebung im On- und Offlinebetrieb gearbeitet und gleichzeitig können in einem zweiten Compartment öffentliche Netzwerke genutzt werden. Die beiden Benutzerumgebungen sind komplett voneinander getrennt und die Informationen im vertrauenswürdigen Compartment bleiben jederzeit geschützt.

Das Herzstück der Hardware besteht aus dem Crypto SmartProtect Security Module. Darauf befinden sich das Boot image des Crypto SmartProtect OS sowie sämtliche Chiffrier- und Authentifizierungsservices. All diese Sicherheitselemente werden durch die Crypto-Sicherheitsarchitektur umfassend geschützt und sind dadurch nicht angreifbar. So kann man die grundlegenden Sicherheitsziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität garantieren. Dazu gehören bewährte Features wie Secure boot, Secure login sowie Disk encryption. Ersteres führt bei jedem Start eine umfassende Sicherheitsprüfung durch. Der Startvorgang wird nur fortgesetzt, wenn diese Prüfung die Unversehrtheit der gesamten Hard- und Software bestätigt. Das zweite Feature, Secure login, garantiert durch eine Multifaktor-Authentisierung einen zweifelsfreien Identitätsnachweis. Schliesslich sorgt die Disk Encryption für eine automatische und permanente Verschlüsselung sämtlicher Daten. Je nach Anwendungsbedarf kann das Crypto SmartProtect Security Module mit der IP-VPN-Chiffrierung oder File-Chiffrierung erweitert werden.

Zurück zum beschriebenen Szenario: Der Einsatz von Crypto SmartProtect ermöglicht dem Mitarbeitenden, Daten auf seinem Rechner gleichzeitig in unterschiedlichen Sicherheitszonen in konsequent getrennten Compartments zu erstellen, bearbeiten, speichern, löschen und übermitteln – und trotzdem kann auf öffentliche Netzwerke zugegriffen werden. Der Mitarbeitende arbeitet so in seiner vertrauten und absolut sicheren Benutzerumgebung, ohne dass er Abstriche im Bedienkomfort hinnehmen muss oder im Datenhandling durch die restriktiven Sicherheitsvorkehrungen eingeschränkt wäre. Tasks können nicht nur hochsicher, sondern auch effizient und komfortabel erledigt werden.

Die Crypto SmartProtect-Computing-Plattform besteht aus Benutzerumgebungen in isolierten Compartments, einem Sicherheits-Betriebssystem und einer geschützten Hardware



Kernkraftwerke gehören zu den am besten geschützten Industrieobjekten und verfügen über umfassende Schutzkonzepte

Staatlich unterstützte Schutzkonzepte

Störungen und Ausfälle kritischer Infrastrukturen (KI) haben gravierende Folgen. Umso wichtiger sind umfassende Schutzmassnahmen, gerade auch um Cyberrisiken zu minimieren. Mit der «Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken» zeigt die Eidgenossenschaft, wo Handlungsbedarf besteht, und bietet mit staatlichen Organen Hilfestellung für die Betreiber von KI.

Die Infrastrukturen eines Staates sind seine Lebensadern. Ihr einwandfreier und verlässlicher Betrieb garantiert Stabilität, Ordnung und Sicherheit – Grundvoraussetzungen für das reibungslose Funktionieren von Gesellschaft, Wirtschaft und Staat. Besonders im Fokus stehen dabei sogenannte kritische Infrastrukturen (KI) aus den Sektoren Behörden, Energie, Verkehr, öffentliche Sicherheit, Entsorgung, Finanzen, Gesundheit, Nahrung, Industrie sowie Information und Kommunikation. Dem Schutz von KI kommt eine besonders hohe Bedeutung zu. Neben dem rein physischen Schutz ist in der jüngsten Vergangenheit der Schutz vor Cyberrisiken stark in den Vordergrund gerückt.

Laut Schätzungen sind 90 Prozent der wichtigen Infrastrukturbereiche in Industriestaaten von Informationstechnologien (IT) abhängig. Der Einsatz von IT führt einerseits zu grösserer Effizienz, nicht zuletzt dank der Vernetzung unter den verschiedenen Bereichen. Andererseits wächst die Abhängigkeit rasant und die Anfälligkeit gegenüber Störungen und Manipulationen nimmt zu. Insgesamt also sind Wirtschaft, Gesellschaft, ja ganze Staaten verwundbarer geworden, womit der Bedarf an effektiven Schutzmassnahmen in der Informationssicherheit steigt. Durch die komplexen, digitalen Vernetzungen der verschiedenen Bereiche genügt es heute jedoch nicht mehr, diese separat zu schützen. Vielmehr sind integrale Schutzkonzepte nötig, um im Schadensfall die Auswirkungen auf Wirtschaft und Bevölkerung möglichst gering zu halten und so rasch wie möglich den Normalzustand wiederherzustellen.

Angriff auf die Informationssysteme
In der 2012 von der Schweizerischen Eidgenossenschaft verabschiedeten «Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken» heisst es: «Cyber-Angriffe auf kritische Infrastrukturen können besonders gravierende Folgen haben, weil sie lebenswichtige Funktionen beeinträchtigen oder fatale Kettenreaktionen auslösen können. Den (oft privaten) KI-Betreibern kommt deshalb eine besondere Bedeutung zu, als Erbringer von wichtigen Leistungen mit übergeordneter, sicherheitsrelevanter Bedeutung.»

Cyberattacken werden auf Computer, Netzwerke und Daten verübt. Ziele solcher Angriffe sind es, die Integrität der Daten oder die Funktionsweise der Infrastruktur zu stören sowie deren Verfügbarkeit einzuschränken oder zu unterbrechen. Unter anderem wollen die Angreifer die Vertraulichkeit oder Authentizität der Informationen beeinträchtigen, indem sie mit ihren Aktionen Daten lesen, löschen oder verändern, Verbindungen oder Server-Dienstleistungen überlasten, Informationskanäle ausspionieren oder Überwachungs- oder Abwicklungssysteme gezielt manipulieren.

> 90 Prozent der wichtigen Infrastrukturbereiche sind von IT und geschützter Kommunikationstechnologie abhängig.

Die Auswirkungen einer Cyberattacke könnten auch für die gesamte Bevölkerung und die Wirtschaft verheerende Folgen haben. So würde nach einer Cyberattacke ein Blackout in der Stromversorgung kritische Infrastrukturen wie auch die gesamte Volkswirtschaft lahmlegen. Auswirkungen davon wären für die Bevölkerung beispielsweise der Ausfall von Beleuchtung, Heizungen und anderen elektronisch gesteuerten Gebrauchsgegenständen, die aus unserem Alltag nicht mehr wegzudenken sind.

Bewusstsein für Cyberrisiken schärfen
In der Strategie wird die Haltung vertreten, dass die einzelnen Akteure grundsätzlich selbst für die Schutzmassnahmen vor Cyberrisiken und deren Optimierung verantwortlich sind. Für die Betreiber von KI bedeutet dies laut Strategie: Die Risiken dürfen nicht nur nach rein ökonomischen Prinzipien gehandhabt werden, sondern die KI-Betreiber müssen darüber hinausgehend Anstrengungen zur Minimierung der Risiken unternehmen.

In einigen Branchen fehlt allerdings nach wie vor das Bewusstsein dafür, welche Bedrohungen von Cyberrisiken ausgehen, schreibt der Bund. Auch ist die integrale Denkweise noch nicht überall etabliert – sprich der Ansatz, dass Cyberrisiken nicht nur mit technischen Massnahmen wie ausfallsicheren, alternativen und speziell geschützten Kommunikationsmitteln reduziert werden können und Informationen und Daten explizit geschützt werden müssen, sondern dass auch organisatorische (wie die Klassifizierung von Informationen oder die Regelung von Zugriffsrechten) und personelle Fragen (unter anderem Sicherheitsprüfungen oder Verhaltensschulungen) von Bedeutung sind.

Staat leistet subsidiäre Hilfe
Zur Rolle des Bundes beim Schutz vor Cyberrisiken heisst es in der Strategie: «Der Staat erbringt subsidiär Leistungen zum Schutz vor Cyberrisiken, zum Beispiel durch Informationsaustausch und nachrichtendienstliche Erkenntnisse.» Eine zentrale Rolle spielt dabei die Melde- und Analysestelle Informationssicherung (MELANI). MELANI wird gemeinsam vom Informatiksteuerungsorgan des Bundes (ISB) und dem Nachrichtendienst (NDB) betrieben.

Die Aufgabe des Organs ist die subsidiäre Unterstützung der kritischen Infrastrukturbetreiber beim Informationssicherungsprozess, indem es Informationen über Vorfälle und Bedrohungen sammelt, auswertet und die daraus gewonnenen Erkenntnisse an die KI-Betreiber weitergibt. MELANI bietet unter anderem Lageeinschätzungen und Analysen zur Früherkennung von Angriffen oder Vorfällen an, wertet deren Auswirkungen aus und untersucht bei Bedarf Schadprogramme.

MELANI unterstützt damit den Risikomanagement-Prozess der kritischen Infrastrukturen und trägt so dazu bei, deren Widerstandskraft (sog. Resilienz) zu stärken. Insgesamt setzt sich die Resilienz kritischer Infrastrukturen aus vier Bausteinen zusammen: aus der Robustheit der Systeme, der Verfügbarkeit von Redundanzen, der Fähigkeit, wirksame Hilfsmassnahmen zu mobilisieren, sowie aus der Schnelligkeit und Effizienz der Hilfsmassnahmen im Ernstfall.

Die weiter zunehmende Digitalisierung und Automatisierung sowie die Vereinheitlichung der verwendeten Technologien (beispielsweise die Konzentration auf IP-Protokolle) wird jedoch neue und zusätzliche Gefährdungen mit sich bringen. Die betroffenen Branchen sind dazu aufgefordert, die möglichen neuen Risiken in der Entwicklung von Systemen, Produkten und der Gestaltung ihrer Prozesse zu berücksichtigen. Gleichzeitig – so schreibt der Bund – ist ein absoluter Schutz vor Cyberattacken nicht umsetzbar. Umso wichtiger ist eine gut funktionierende und weitsichtige Zusammenarbeit zwischen Behörden und Betreibern kritischer Infrastrukturen, um auf real werdende Cyberbedrohungen schnell und sicher reagieren zu können und die notwendigen Grundlagen für ein geschütztes und widerstandsfähiges Informationssicherheitssystem zu ermöglichen.

Blackout in einer Grossstadt – möglicherweise durch eine Cyberattacke ausgelöst

Sicher kommunizieren via Chat

Sprach- und Textnachrichten gehören schon seit längerer Zeit zum Alltag. Seit einigen Monaten bieten Anbieter von Messaging-Applikationen nun den geschützten Austausch von Nachrichten an. Wie funktionieren diese und wie sicher sind sie? Aufgezeigt wird auch, welche hochsichere Lösung die Crypto AG zu diesem Thema anbietet.

Das Thema Verschlüsselung ist in aller Munde, seit verschiedene Anbieter von Messaging-Applikationen ihre Dienste mit sogenannten End-zu-End-Verschlüsselungen zur Verfügung stellen. In den jeweiligen Beschreibungen zur angepriesenen Applikation steht, dass weder Anbieter noch Dritte die jeweiligen Nachrichten lesen können. Gemäss Anbieter sei die Verschlüsselung für alle Personen verfügbar, die die aktuellste Applikationen-Version verwenden.

Das Szenario für das Versenden von verschlüsselten Nachrichten sieht folgendermassen aus: Der Empfänger erzeugt zunächst ein eigenes Schlüsselpaar. Der öffentliche Schlüssel wird über den Server dem Sender mitgeteilt, damit dieser damit die Nachricht verschlüsseln kann. Mit dem eigenen privaten Schlüssel kann der Empfänger dann die Nachricht entschlüsseln. Eine mögliche Schwachstelle ist jedoch, dass der Anbieter beispielsweise bei einem Gerätewechsel oder einer Neuinstallation dem Sender einen neuen öffentlichen Schlüssel zuweisen kann. Der Sender würde dann beispielsweise Nachrichten, die noch nicht beim Empfänger angekommen sind, mit dem vom Anbieter erzeugten Schlüssel chiffrieren. Damit würde der Anbieter in die Lage versetzt, die Nachrichten mit seinem neuen privaten Schlüssel zu dechiffrieren.
Weiter können auch die Endgeräte selbst mögliche Einfallstore aufweisen. Schlüsselbegriffe wie fehlender Integrationsschutz der Anwendung, fehlender echter Zufallszahlengenerator oder auch zu kurze Schlüsselpaare weisen darauf hin.

Verschlüsselter Chat der Crypto AG
Die Crypto AG bietet schon seit einigen Jahren mit einem speziell gehärteten Mobiltelefon eine attraktive und hochsichere Kommunikationslösung an. Gehärtet bedeutet, dass eine unautorisierte Modifikation des Gerätes sofort angezeigt wird. Sprach- und Textnachrichten sind mit dem Crypto Mobile HC-9100 jederzeit und überall geschützt.

Der Kunde betreibt seine Infrastruktur autonom, womit seine Daten immer unter seiner Kontrolle sind. Die Verschlüsselung geschieht durch das gehärtete Mobiltelefon in einer sicheren Hardwareumgebung, in der der Kunde seinen eigenen Chiffrieralgorithmus nutzt. Nur der Kunde allein besitzt und verwaltet seine Schlüssel, die mit einem True-Random-Generator erzeugt wurden.

> Sprach- und Textnachrichten sind mit dem Crypto Mobile HC-9100 jederzeit und überall geschützt.

Für den Austausch von Textnachrichten wird die bis zu 1'000 Zeichen lange Nachricht direkt in dem im Telefon integrierten, weltweit kleinsten High-Security-Chiffriergerät chiffriert und direkt an den Empfänger übermittelt. Der Absender erfährt umgehend, dass die Nachricht beim Empfänger angekommen ist. Sobald die Nachricht der Sicherheitsapplikation übergeben wird, ist die Sicherheit nicht nur bei der Übermittlung, sondern auch in den beiden Endgeräten gewährleistet. Die Nachricht wird im Secure Data Store des HC-9100 gespeichert, und zwar ausschliesslich im sendenden und empfangenden Gerät. Dadurch unterscheidet sich die hochsichere Lösung massgeblich von den handelsüblichen Angeboten.

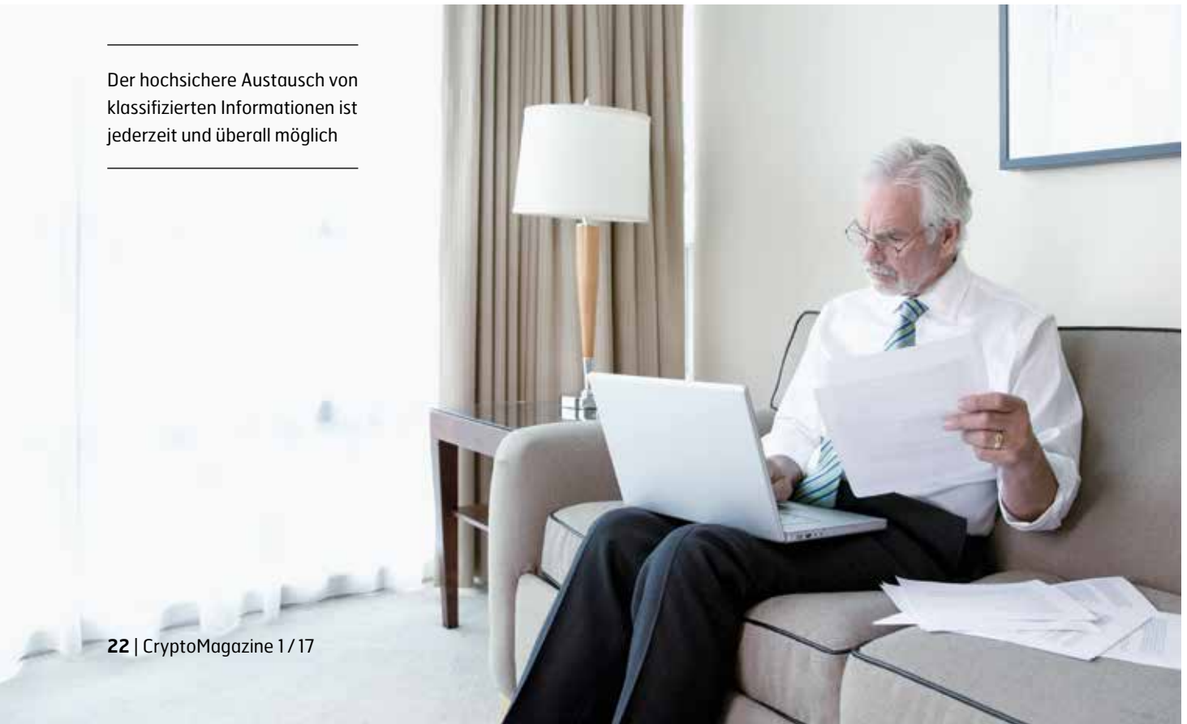
SUCCESS STORY

End-zu-End-geschützter Dokumentenaustausch im Regierungsumfeld

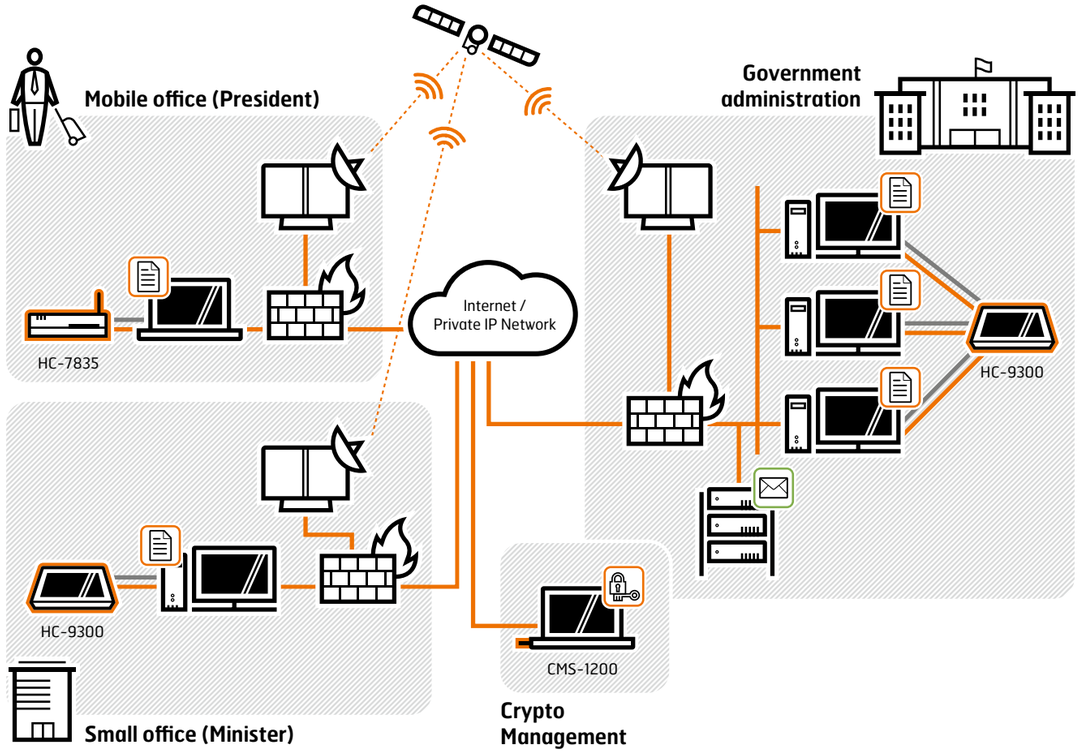
Ein Minister ist darauf angewiesen, dass die sichere Kommunikation zwischen ihm und seinem Mitarbeitendenstab sowie den Vorstehern der verschiedenen Ministerien vor Dritten kompromisslos geschützt und permanent gewährleistet ist. Ein auf höchstem Niveau verschlüsselter Austausch editierbarer Dokumente erfüllt diese Anforderungen.

Die Zusammenarbeit mit verschiedenen Stellen in einem Ministerium gestaltet sich vielfältig: Der Minister wird von seinem Stab bei der Ausübung seiner politischen Aufgaben unterstützt, Dienststellen des jeweiligen Ministeriums müssen beaufsichtigt werden, aber auch alltägliche Verwaltungsaufgaben wollen erfüllt sein. Bei der Ausübung all dieser Aufgaben muss die hochsichere Übermittlung von klassifizierten Dokumenten und Informationen permanent für alle Mitarbeitenden sichergestellt sein. Abhängig vom Aufenthaltsort der jeweiligen Personen kommt dabei die dafür geeignete Sicherheitsplattform zum Einsatz. Das zentrale Sicherheitsmanagement zur Verwaltung der Kommunikationsbeziehungen und Benutzer (-gruppen) ist dabei essenziell.

Hochsicherer Austausch editierbarer Dokumente
Für die hochsichere Kommunikation vom stationären oder mobilen Büro eines Staatsoberhauptes zur Regierungsadministration oder den Ministern kann das Internet oder aber auch ein privates IP-Netzwerk verwendet werden. Durch den weltweiten Ausbau der Datennetze und der damit einhergehenden Leistungsfähigkeit hat sich die IP-Telefonie durchgesetzt.
Die vertrauliche Übermittlung von chiffrierten, editierbaren Dokumenten via E-Mail wird mit dem Einsatz der Multiapplikations-Plattform Crypto Desktop HC-9300 und der Sicherheitsapplikation Message / File Encryption HA-6650 sichergestellt.



Der hochsichere Austausch von klassifizierten Informationen ist jederzeit und überall möglich



Die hochsichere Kommunikation vom stationären oder mobilen Büro über Internet oder ein privates IP-Netzwerk ist permanent gesichert

Auch von unterwegs kann der Minister mit dem Crypto Mobile Client HC-7835 Daten verschlüsseln und sicher an seine Mitarbeitenden versenden. Mit der Crypto Management Suite CMS-1200 wird das zentralisierte Sicherheitsmanagement der Crypto-Plattformen gewährleistet. Weiter verfügt das CMS-1200 über ein massgeschneidertes Benutzer- und Berechtigungsmanagement mit Authentifizierungsmechanismen.

> Die hochsichere Übermittlung von klassifizierten Dokumenten und Informationen muss für alle Mitarbeitenden permanent sichergestellt sein.

Für die ständige Verfügbarkeit und Ausfallsicherheit kann bei Bedarf ein auf Satellitenkommunikation basierender Backup-Kommunikationskanal eingerichtet werden. Das Deployable Secure Mobile Office bietet hier eine kompakte Büroinfrastruktur, die an jedem beliebigen Standort mittels Satellitenkommunikation betrieben werden kann und die gewohnten Bürokomponenten umfasst.

Die Crypto AG bietet hiermit eine auf höchste Ansprüche ausgerichtete Sicherheitslösung für die End-zu-End-geschützte Kommunikation und Kollaboration.

Crypto cSeminars

cSeminar Information Security Specialists
2. bis 6. Oktober 2017

cSeminar Technical Vulnerability Testing
9. bis 13. Oktober 2017

cSeminar Contemporary Cryptography
16. bis 20. Oktober 2017

Die Seminare finden in der Crypto Academy
in Steinhausen / Zug, Schweiz, statt.

Kontakt und weitere Informationen unter
www.crypto.ch/seminars

Crypto AG
Postfach 460
6301 Zug
Schweiz
T +41 41 749 77 22
F +41 41 741 22 72
crypto@crypto.ch
www.crypto.ch