Rüstung und Technik

Von Siemens zu Atos

Der Ausbau des schweizweiten Polycom-Netzes schreitet wie geplant voran. Mit Ausnahme des Kantons Zug haben sich inzwischen alle Kantone für Polycom entschieden. Es wird damit gerechnet, dass sich Zug in absehbarer Zeit in die Polycom-Familie integrieren wird.

OBERSTLT PETER JENNI BERICHTET VOM POLYCOM-TAG IN SCHWARZENBURG

Am 9. November 2011 fand der traditionelle Polycom-Day statt. Einige hundert Angehörige der Polizei, der Sanität, der Katastrophenhilfe, der Feuerwehr und der Behörden aus der ganzen Schweiz fanden sich bei schönstem Wetter im bernischen Schwarzenburg zum Informationsanlass ein. Der Anlass wurde bisher von Siemens Schweiz AG organisiert. Neu nun von Atos IT Solutions and Services AG.

Zusammenschluss

Der Head of Public Security, Civil and National Security von Atos, Justus Bernold, informierte die Anwesenden über den Zusammenschluss. Ein Thema, das die Polycom-Gemeinde stark interessierte.

Am 1. Oktober 2010 siedelte die Siemens Schweiz AG den Bereich IT in das Tochterunternehmen Siemens IT Solutions and Services AG (SIS) aus. Zu Beginn des Monats Juli 2011 erfolgte der Zusammenschluss der SIS und der Atos Origin. Damit sind die früheren Siemens-Mitarbeiter Teil des französischen Konzerns Atos.

Er ist global tätig, beschäftigt fast 80 000 Mitarbeitende und erzielte im vergangenen Jahr einen Umsatz von 8,7 Milliarden Franken. Der Konzern ist in 42 Ländern aktiv und in Europa gemäss eigenen Angaben der führende Anbieter von IT-Diensten. Siemens ist mit 15 Prozent Aktienanteil an Atos beteiligt.

Kernkompetenzen

Justus Bernold unterstrich, dass sich für die Kunden im Bereich Civil and National Security und Polycom nichts ändern werde. Die vorhandenen Kompetenzen seien für Atos bedeutsam und würden nicht nur weitergeführt, sondern ausgebaut. Der Hauptsitz verbleibt in Zürich. Die übrigen Standorte sind Reinach, Bern, Renens, Lausanne und Vevey. Gegenwärtig stehen in der Schweiz rund 520 Mitarbeitende im Dienst von Atos.

Die Kernkompetenzen der neuen Firma umschrieb Justus Bernold wie folgt:

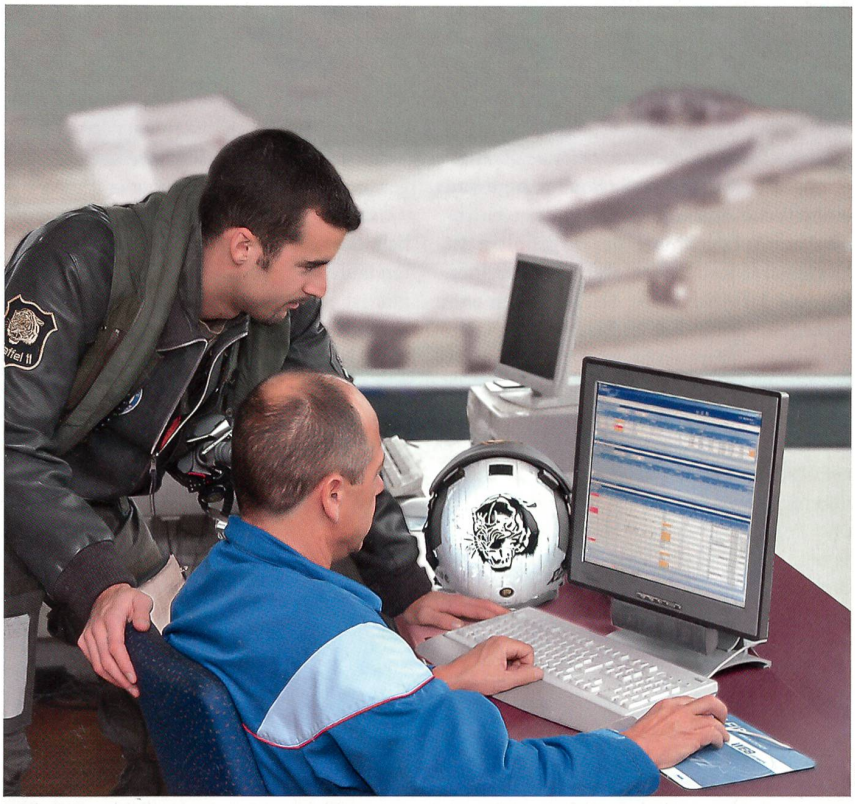


Bild: Atos

Das CCIS AF von Siemens wird in Zukunft von Atos unterstützt. Es ist als Führungsinformationssystem der Luftwaffe (FIS LW) bei der Schweizer Luftwaffe seit 2002 im Einsatz. Als Integrationsplattform stellt FIS LW die Durchgängigkeit über alle Stufen sowie in allen Lagen sicher.

Sie liegen in den Bereichen Notfallmanagement für die Polizei, Sanität, Feuerwehr, für die Armee auf dem Gebiet Command and Control, im professionellen Funk (PMR) und in sicheren Netzwerken für die Daten und Sprachkommunikation. Das weltweite Kompetenzzentrum von Atos mit PMR liegt in der Schweiz.

Das Polycom-Haus

Grundsätzlich wurde in Schwarzenburg festgehalten, dass das Polycom-Haus kaum je fertig gebaut sein wird. Heute sind weltweit über eine Million Endgeräte mit dem Standard Tetrapol im Einsatz. In der Schweiz sind es 2011 40 000 Geräte. Bis 2015 dürfte diese Zahl auf 50 000 steigen.

Gearbeitet wird im Moment am Projekt «Schweiz dunkel», das heisst, es gilt die Stromversorgung für den Betrieb des Netzes sicherzustellen. Bis 2015 ist geplant, «Polyalert», die Alarmierung in der Schweiz via Sirenen und elektronische Medien, zu garantieren.

Oberstlt Peter Jenni, Muri bei Bern, ist Rubrikredaktor Rüstung + Technik des SCHWEIZER SOLDAT. Er kennt die nationale und internationale Rüstungsindustrie profund. Immer wieder berichtet er von Flugmeetings.

Realitätsnahe Simulatoren

Komplexe Waffensysteme erfordern eine intensive Schulung. Vor dem praktischen Einsatz vermitteln Simulatoren den Soldaten Grundwissen und -fähigkeiten.

OBERSTLT PETER JENNI BERICHTET IN WORT UND BILD AUS MANCHING

Die Schulung an Simulatoren ist heute im Militär für Schiesstrainings, für die Besatzung von Kampf- und Schützenpanzern, die Gefechtsausbildung, die taktische Schulung sowie für Kampfjet- und Helikopterpiloten integraler Bestandteil der Ausbildung.

Das Üben mit Simulatoren ist kostengünstig, belastet die Umwelt weniger und ermöglicht eine qualitativ hochwertige und einheitliche Ausbildung. Dank der elektronischen Aufzeichnung der Ergebnisse ist zweifelsfrei feststellbar, wer die einzelnen Module der Ausbildung den Vorgaben entsprechend erfüllt hat und wer zum «Nachexerzieren» antreten muss.

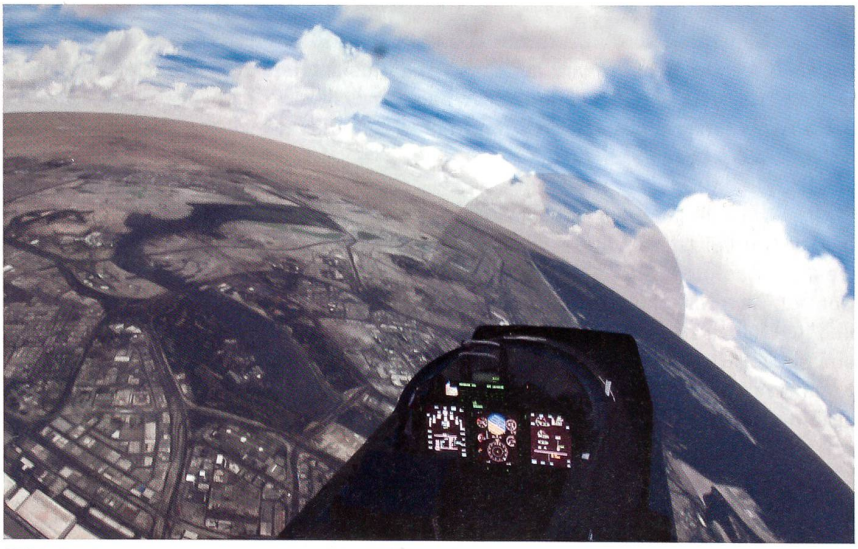
Prunkstück ASTA

Die europäische Firma Cassidian – sie gehört zum Konzern EADS und ist unter anderem verantwortlich für die Entwicklung und Produktion des Kampfflugzeugs Eurofighter – hat in ihrem Portfolio verschiedenste Typen von Simulatoren, zum Beispiel für das Training von Wartungsspezialisten des Eurofighters oder des Kampfhelikopters Tiger, für die Piloten des Eurofighters oder für Trainingsflugzeuge, wie beispielsweise der PC-21 aus Stans. Die Prunkstücke im Angebot sind zweifelsfrei die sogenannten Eurofighter ASTA (Aircrew Synthetic Training Aids) Missionssimulatoren und die ASTA-Cockpit-Trainer. Sie basieren auf den modernsten Simulationstechnologien und wurden dem Schreibenden vom ehemaligen Piloten Erik Heinzmann in Manching begeistert vorgestellt.

Erik Heinzmann ist dafür verantwortlich, dass die Anliegen der Luftwaffenpiloten laufend in die Software einfliessen. Damit ist sichergestellt, dass der Simulator aktuell an die Erfahrungen der Praxis angeglichen werden kann.

Im ASTA können die Piloten jener Länder, die am Projekt Eurofighter beteiligt sind, im «Theoriesaal» alles üben, was das System dieser Kampfmaschine ermöglicht, ohne ein Risiko einzugehen. Die in tausenden von Stunden gemeinsam mit Nutzern und Herstellern entwickelte Software bietet dem Piloten eine einzigartige synthetische Welt. Die Schüler erhalten beim Üben das Gefühl, in der Luft zu sein.

Sie sehen und hören während des Fluges ihre Kameraden, bekämpfen den Gegner, finden das Tankflugzeug, mit dem sie das Tanken im Flug trainieren. Das Verhalten in der elektronischen Kriegführung sowie der Überschallflug im Tiefflug gehören selbstverständlich auch dazu.



Blick in das Simulationscockpit des PC-21, das von Cassidian für einen Kunden aus dem arabischen Raum entwickelt worden ist. Im Hintergrund ist ein Teil der arabischen Halbinsel zu sehen.

Auftrag aus Koblenz

Die Simulatorentechnologien sind bereits so weit fortgeschritten, dass die deutsche Luftwaffe danach strebt, nur noch 50 Prozent der Einsätze in der freien Natur trainieren zu müssen. Die anderen 50 Prozent üben die Piloten im Simulator. Das wird aktuell in der Erstausbildung der Eurofighterpiloten praktiziert. Obschon der Simulator alles andere als billig ist, kann mit dieser Aufteilung viel Geld gespart und die Umwelt geschont werden.

Wie Bettina Weber, bei Cassidian für die Eurofighter-Export-Trainingsprogramme verantwortlich, mitteilte, erteilte das Bundesamt für Wehrtechnik und Beschaffung in Koblenz Cassidian, CAE Elektronik GmbH und Rheinmetall Defence Electronics den Auftrag für den Betrieb, die Wartung und Instandsetzung von sechs Simulatoren des Typs ASTA in Deutschland.

Vielseitig angewendet

Neben dem «Ferrari» ASTA kommt für das Erlernen der Funktionen im Cockpit des Eurofighters ein abgespeckter Trainer zum Einsatz. Mit einem erweiterten Simulator lernt der Pilot, mit den Software gestützten Waffensystemen, dem Radar und den zahlreichen Bedien- und Bildschirmfunktionen umzugehen.

Für die Ausbildung des Bodenpersonals des Kampfhelikopters Tiger haben Frankreich und Deutschland gemeinsam bei Cassidian einen Wartungssimulator entwickeln lassen, der in Kürze in den Trainingsbetrieb gehen wird.

Bodenpersonal ausbilden

Für die Logistik und die Wartung des Eurofighters hat Cassidian ein integriertes Schulungsprogramm erstellt, das computergestütztes Training (CBT) und einen Wartungssimulator, den sogenannten

Maintenance Simulation Trainer (MST), umfasst. Die Auszubildenden sitzen im Schulungsraum, vor sich Computerbildschirme, und an die Wand des Raumes wird das Bild vom Trainer auf eine grosse Leinwand projiziert.

Der Lehrer kann mit Hilfe des CBT die Details des Flugzeugaufbaus mit den verschiedenen Funktionen und die Zusammenhänge und Abhängigkeiten erklären. Die Schüler lernen anschliessend auf ihren Bildschirmen selbständig das Funktionieren des Systems. In einem weiteren Schritt geht es darum, Fehler in Echtzeit zu beheben, die am MST simuliert werden. Sie werden vom Trainer eingebaut.

Von jedem Auszubildenden gibt es einen Datensatz, in dem die Fortschritte oder Rückschläge festgehalten sind. Die Entwicklung dieses Programms beanspruchte gemäss Günter Stadler, Leiter Programm-Management neue Trainingssysteme, einige Jahre. Es wird heute von allen vier Nationen (Deutschland, Grossbritannien, Italien, Spanien) genutzt.

Simulatoren für PC-21

Nicht unerwähnt bleiben dürfen die zwei PC-21-Simulatoren und ein Schulungsraum, die Cassidian in nur 20 Monaten für einen Kunden aus dem arabischen Raum entwickelt hat und nun produziert. Das Programm wird 2012 abgeschlossen werden.

Der PC-21-Simulator besteht aus einem 9-Kanal-Sichtsystem und einem originalgetreuen Cockpit mit beweglichem G-Sitz. In der Datenbasis sind unter anderem 1,8 Millionen Quadratmeter der arabischen Halbinsel detailgetreu abgebildet. Der Simulator ist für die Nachtflugausbildung mit Bildverstärkerbrillen geeignet.

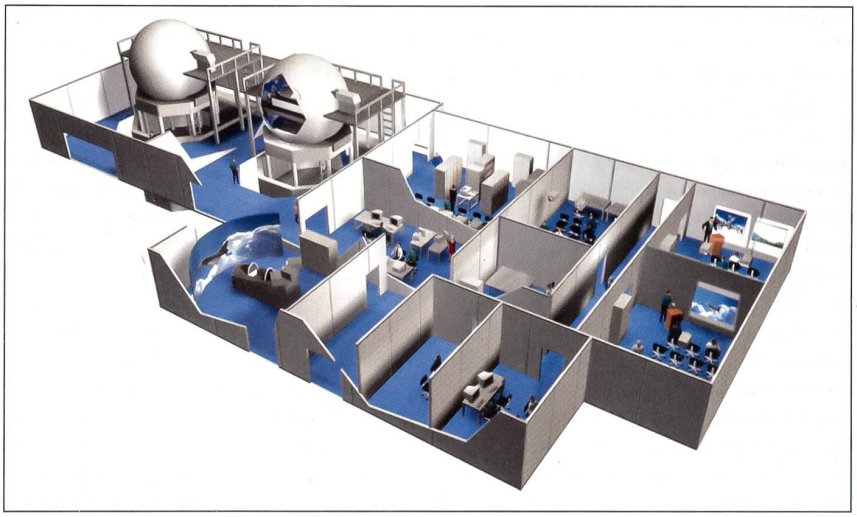
Sprengmittel entschärfen

Für die Beseitigung von vermuteten mit Sprengstoff gefüllten Paketen, Koffern, Metallboxen und Rohrbomben setzt die Polizei und die Armee ferngesteuerte Roboter ein. Ein verbreitet im Einsatz stehender Roboter ist der tEODor von der Firma telerob. Er wurde zur Erkundung und Eliminierung von Sprengfallen, Brandvorrichtungen, Minen oder sonstigen Kampfmitteln gebaut.

Das Lenken eines Roboters aus sicherer Entfernung bedarf der Übung. Cassidian hat für diesen Zweck den tEODor SIM 2.0 Simulator entwickelt. Der Übende sieht auf dem Bildschirm eine nachgebildete Umgebung, die je nach Bedürfnissen des Kunden gestaltet werden kann. Der Schüler weiss ungefähr, wo sich das gefährliche Objekt befindet, und steuert den Roboter über Hindernisse und schlechten Untergrund dorthin. Sobald er es dank der Kamera auf dem Roboterarm sieht, lenkt er den Greifarm zum Erfassen des Objekts und bringt es an einen sicheren Ort. Dies tönt einfach, ist aber in der Praxis heikel und muss vorher intensiv geübt werden. Nur so können alle Werkzeuge und Abläufe in unterschiedlichsten Orten und Szenarien beherrscht werden.

Bild: EADS

Mit dem Wartungssimulator werden die auszubildenden Techniker mit dem System Eurofighter im Detail vertraut gemacht.



Auf der Grafik sind links die «Kugeln» mit den Missionssimulatoren für den Eurofighter und davor der kleinere Cockpittrainer zu sehen. In der Mitte überwachen und steuern die Instruktoren das Training. Diese Einrichtungen, zusammen mit den Computern und Debriefungsräumen, sind in einem besonderen Gebäude untergebracht.

Welcher Zünder?

Die Sicherheitsorgane stehen bei Sprengstoffpaketen meistens vor der heiklen Frage, um welchen Zünder und welchen Sprengstoff es sich wohl handelt. Cassidian kann den Experten ein transportables Hilfsmittel zur Verfügung stellen, mit dem vor Ort Röntgenbilder von Sprengfallen mit Bildern abgeglichen werden, die im Gerät gespeichert sind. Hunderte IED-Bauteile (IED: Improvised Explosive Devices = Sprengfallen) sind in verschiedenen Blickwinkeln und mit technischen Angaben in der Datenbank hinterlegt.

Der Fachmann sieht sofort, um welchen Zündmechanismus es sich handelt. Mit einer integrierten digitalen Tafel (Whiteboard) kann er die einzelnen Komponenten der Sprengfalle virtuell zu einem Schaltkreis zusammensetzen. Dieses Wissen erleichtert die weiteren Schritte bei der Unschädlichmachung des Objektes.

Ist die Schweiz gewappnet?

An ihrer Herbstveranstaltung vom 3. November 2011 beschäftigte sich die Schweizerische Gesellschaft Technik und Armee (STA) bereits zum zweiten Mal in Folge mit dem Thema Cyberwar. Die Frage lautete, ist die Schweiz gegen diese Herausforderung gewappnet.

OBERSTLT PETER JENNI BERICHTET VON DER HERBSTTAGUNG DER STA

Wie aktuell und bedrohlich das Thema ist, bewies der am 31. Oktober 2011 veröffentlichte Halbjahresbericht der Melde- und Analysestelle Informationssicherheit des Bundes Melani.

Er hielt fest, dass weltweit vermehrt Spionageangriffe auf verschiedenste Unternehmen festgestellt worden sind. Gestiegen sind ebenfalls die Hackerangriffe mit dem Ziel, an sensible Daten zu gelangen. In der Schweiz hat sich ferner die Anzahl der sogenannten Skimmingfälle stark erhöht.

Netzinfrastruktur

Fast alle kriminellen Machenschaften im Internet haben das primäre Ziel, finanzielle Gewinne zu generieren. Um an die vertraulichen Daten zu gelangen, nutzen die Angreifer die Gutmütigkeit und Hilfsbereitschaft der Opfer aus, indem sie ihnen zum Beispiel E-Mails mit gefälschten Absenderadressen zustellen, um so an die gesuchten Daten zu kommen.

Die Verantwortlichen von Melani stellen ferner fest, dass mittlerweile jeden Tag versucht wird, in Firmennetze zu gelangen, um diese auszuspionieren.

Fritz Gantert, Präsident der STA, hielt im Anschluss an die Begrüssung der zahlreich erschienenen Gäste aus Wirtschaft, Behörden und Militär fest, dass der Anlass eine vertiefte Fortsetzung des Anlasses zum selben Thema aus dem Jahr 2010 sei.

Er wies darauf hin, dass unsere Gesellschaft als Teil einer zunehmend vernetzten Welt in grossem Mass abhängig von einer störungsfrei funktionierenden Netzinfrastruktur sei. Auf diesen Netzen liefen immer mehr kritische und sicherheitsrelevante Applikationen, die für das Funktionieren von Wirtschaft und Gesellschaft von vitaler Bedeutung seien.

Die rasanten Fortschritte in den Informations- und Kommunikationstechnologien eröffneten laufend neue Nutzungsmöglichkeiten. Die Entwicklung in die Abhängigkeit dieser Technologien schaffe neue Verwundbarkeiten und reale Gefahren für das Funktionieren unserer Gesellschaft.

Was tut die Schweiz?

Der Chef der Armee, Korpskommandant André Blattmann, hat vor kurzem festgehalten, dass heute die Gefahr des Cyberkriegs die Bedrohung unseres Landes sei. Dominik Schwerzmann, Fachreferent im Generalsekretariat des VBS und Mitglied des Projektteams Cyber Defence, erläuterte in seinem Vortrag den Stand der Arbeiten auf Stufe Bund am Projekt Cyber Defence. Er stellte fest, dass die Wahrnehmung des Cyber-Risikos noch relativ jung ist. Nach dem Beginn der IT-Revolution Anfang der achtziger Jahre des letzten Jahrhunderts bestanden gewisse Befürchtungen wegen eines möglichen Cyber Pearl Harbor.

Es zeigte sich aber, dass die damaligen Beurteilungen und Wahrnehmungen die Gefahren überschätzten. Real wurden die Risiken nach dem Jahr 2000. Man erinnert sich an die Vorkehrungen bei Behörden und Wirtschaft in der Nacht vom 31. Dezember 1999 auf den 1. Januar 2000, die rückblickend übertrieben waren. Die damaligen Befürchtungen traten glücklicherweise nicht ein.

Die Wahrnehmung

Heute habe man das Gefühl, dass die nun real vorhandenen Bedrohungen in den Informationstechnologien vielerorts nicht rechtzeitig wahrgenommen worden seien. Immerhin hat der Bundesrat das VBS beauftragt, eine Strategie gegen die Cyber-Risiken zu erarbeiten; das Dokument soll demnächst fertiggestellt sein. Es muss Auskunft darüber geben

- Wie die Bedrohungslage im Cyberspace aussieht
- Wie der Bund und die Schweiz bzw. die Betreiber der kritischen Infrastrukturen dagegen gerüstet sind
- Wo die Mängel liegen und
- Wie diese Mängel am effektivsten und effizientesten zu beheben wären.

Kritische Struktur

Miteinbezogen in diese Arbeiten seien:

- Die Wirtschaft als Nutzer und Versorger kritischer Infrastrukturen, als Dienstleister, Hersteller und Lieferant.
- Die Betreiber von kritischen Infrastrukturen als Erbringer von Leistungen mit einer übergeordneten und sicherheitsrelevanten öffentlichen Bedeutung.
- Die Behörden von Bund und Kantonen als Betreiber und Nutzer kritischer In-

Erfahrungsaustausch beim Stehlunch: Markus Niederhauser, CEO Systems Assembling SA, Boudry und Peter Müller, Leiter Politik und Forschung Armasuisse.

frastrukuren, als Gesetzgeber und Richter (inkl. Strafvollzug), Aufsichtsbehörden und Dienstleister als Risiko- und Krisenmanagementorgane sowie die Betreiber von Forschungs- und Entwicklungseinrichtungen.
- Die Bevölkerung. Sie nutzt Infrastrukturen und Dienstleistungen, betreibt und nutzt privat und geschäftlich IKT Systeme.

Herausforderungen

Die Herausforderungen, die sich dem Projekt Cyber Defence stellen, sind nach Dominik Schwerzmann vielfältig. Obschon die Schweiz eher klein sei, verfüge sie über renommierte Universitäten, Hightech-Firmen und eine bedeutende Finanzindustrie.

Die Globalisierung mit ihrer Vernetzung habe auch vor diesen Institutionen nicht halt gemacht. Hier liege eine grosse Gefahr wegen Spionage und Sabotage. Die Interessen der sieben Departemente, der 26 Kantone und weiterer Akteure stimmten nicht immer überein.

Es komme hinzu, dass die staatlichen Sicherheitsinteressen mit marktwirtschaftlichen und persönlichen Interessen kollidierten. Wie weit sollten Anreize zum Handeln und zur Zusammenarbeit verordnet oder freiwillig erfolgen? Wer trage die Verantwortung und die Kosten? Daran anschliessend stelle sich die Frage der Neutralität der Schweiz.

Wo kommen Angriffe?

Angriffe sind für Dominik Schwerzmann denkbar auf die Kommunikationswege, sprich Übertragungseinrichtungen wie Kabel und drahtlose Transportmöglichkeiten via Satelliten, und auf die Daten, die in Rechnern gespeichert sind.

Angesichts der geringen Kosten einer Attacke bestehe für den Angreifer ein günstiges Kosten-Nutzen-Verhältnis. Er könne Distanzen und Grenzen ohne Kontrolle und dank der Zunahme der technischen Leistungsfähigkeiten leicht überwinden.

Die grössten Gefahren lägen in den wachsenden Abhängigkeiten, der Vernetzung, der Komplexität und der Intransparenz der ganzen Informationstechnologie. Die Cyber-Bedrohungen, denen die Schweiz täglich ausgesetzt sei und die das Funktionieren von Wirtschaft, Gesellschaft und Insitutionen permanent und nachhaltig beeinträchtigten nähmen laufend an Intensität und Komplexität zu.

Sie würden durch fahrlässiges Verhalten, fehlerhafte technische Entwicklungen und unzureichende Sicherheitskonzepte begünstigt. Für Dominik Schwerzmann gibt es angesichts der aufgezeigten Herausforderungen keinen absoluten Schutz.

Bestandesaufnahme

Die Arbeiten im Projekt Cyber Defence hätten gezeigt, dass in der Schweiz die vorhandenen Fähigkeiten unzureichend koordiniert und verstreut seien. Die vorhandenen Gegenstrategien seien auf die normale Situation ausgerichtet und nicht auf die sicherheitspolitischen Bedürfnisse der Schweiz als Ganzes. Sie zeigten wenig Verständnis für und Wissen über die Komplexität der Herausforderung.

Die meisten Konzepte befassten sich nur mit der Computer-Sicherheit. Es gelte, in der Schweiz auf dem Gebiet der Informationstechnologie eine Sicherheitskultur zu entwickeln, die alle Mitspieler akzeptierten.

Lösungsansatz

Dominik Schwerzmann legte schliesslich dar, woran gearbeitet werden muss. Es gehe darum, die vorhandenen Kräfte zu bündeln. Das heisse, die Informationen, die Fähigkeiten und die Massnahmen zu koordinieren. Dazu gehörten der Nachrichtendienst, die Technik, die Strafverfolgungsbehörden, die internationale Zusammenarbeit und die entsprechenden Rechtsgrundlagen. Selbstverständlich müssten diese Schutz- und Vorsorgemassnahmen politisch beaufsichtigt werden.

Die pointierten Aussagen des Sicherheitsforschers an der Freien Universität Berlin, Sandro Gaycken, wirkten wie eine kalte Dusche für die Anwesenden im Saal. Nach den vorherigen Referenten glaubte männiglich, man sei auf gutem Weg und werde die Gefahren sicher einigermassen beherrschen.

Klare Aussagen

Sandro Gaycken erinnerte an den Vorfall in Lettland und stellte fest, dass das keine lebensbedrohende Attacke gewesen sei. Wohl seien während einiger Zeit gewisse Systeme ausgefallen, die Angreifer seien aber im Vergleich mit den zu befürchtenden Angriffen kleine Fische. Die wirkliche Gefahr komme von den staatlichen Nachrichtendiensten, die über gewaltige personelle und finanzielle Mittel verfügten. Diesen gehe es nicht darum, ein System zu lähmen, sondern darum, unerkannt zu wertvollen Informationen zu gelangen. Sie seien gut getarnt und man wisse nicht, wer dahinter stecke.

Diese Eindringlinge strebten an, möglichst nicht feststellbar in einem IT-System zu «leben» und zugunsten des Auftraggebers Informationen zu liefern. Interessant seien dabei Produktionseinrichtungen und Forschungsabteilungen. Die dazu nötige Software sei für fünf bis sieben Millionen Dollar zu haben.

Ungeschützte Börsen

Der Referent wies auch darauf hin, dass die Börsen über keine gegen Unbefugte gesicherte Informatik besässen. Das sei für einen Angreifer ein ideales Spielfeld, mit dem weltweit ungeahntes Unheil angerichtet werden könne.

Mit den jetzt von der Industrie angebotenen Schutzmassnahmen könne gegen die beschriebenen Möglichkeiten von staatlichen Akteuren lediglich ein Schutzgrad von fünf bis zehn Prozent erreicht werden. Das heisse, dass heute kein Schutz, der diesen Namen verdient, möglich sei. Eine Chance, um die Verletztlichkeit zu reduzieren, sei die Verringerung der Komplexität der IT Systeme, zudem solle nicht alles und jedes vernetzt werden.

Sandro Gaycken zeigte sich schliesslich völlig verblüfft über die Idee der Militärs, die Soldaten mit GPS-Geräten auszurüsten. Diese Geräte seien ein leichtes Ziel für einen Angreifer. Er bezeichnete diese Idee geradezu als Idiotie. Eines der am besten geschützten Länder gegen Cyber-Attacken sei Rwanda, weil dort praktisch keine Computer stünden.

Markt für Datenhandel

Den Abschluss der spannenden Veranstaltung bildeten die Ausführungen von Jörg Eschweiler, Head of Sales & Programs Germany Cyber Security von Cassidian. Er ist überzeugt, dass etwas gegen die Bedrohung im Cyber Space getan werden muss.

Aus seiner Sicht bestehe die Gefahr eines Datenklaus unter anderem auf den vielen Reisen, welche die Mitarbeiter heute machen müssen. Es gebe bereits eine Industrie, die Daten klaut, um sie weiter zu verkaufen. Auch er sieht eine Ursache für die Probleme in der Vernetzung. Bei Cassidian darf nicht alles vernetzt werden.

Die unbewusste Vernetzung geschehe häufig durch externe Dienstleister. Um den unterschiedlichen Rechtssystemen der Länder Rechnung zu tragen, habe Cassidian die Reglemente daraufhin angepasst. Keine Nation oder Organisation sei heute in der Lage, die Herausforderung Cyber War selbständig zu bewältigen. Es brauche eine gemeinsame Plattform.

In gewohnt gekonnter Art wurde der Anlass von Peter Forster, Chefredaktor SCHWEIZER SOLDAT, moderiert.