Zeitschrift: Schweizer Soldat : die führende Militärzeitschrift der Schweiz
Herausgeber: Verlagsgenossenschaft Schweizer Soldat
Band: 85 (2010)
Heft: 12

Rubrik: Rüstung und Technik

Bilder: EADS

Der Euro Hawk am 29. Juni 2010 beim Start zum Erstflug vom Fertigungsgelände von Northrop Grumman im kalifornischen Palmdale. Die Maschine stieg auf eine Flughöhe von 32 000 Fuss. Nach knapp zwei Stunden landete der Euro Hawk sicher auf der Edwards Air Force Base in Kalifornien.

Erfolgreicher Erstflug

Das von Northrop Grumman Corporation und EADS Defence & Security (DS) auf der Basis des Global Hawk – einer Drohne der US-Luftwaffe – gebaute UAS (Unmanned Aerial System – unbemannt fliegendes System) Euro Hawk hat in Kalifornien den Erstflug erfolgreich absolviert.

Den Auftrag für die Entwicklung, Erprobung und Unterstützung des unbemannten Aufklärungssystems Euro Hawk hatte das deutsche Verteidigungsministerium am 31. Januar 2007 der EuroHawk GmbH erteilt.

Die Firma wurde von Northrop Grumman und EADS DS als Joint Venture mit gleicher Beteiligung gegründet. Die Firma ist gegenüber dem deutschen Verteidigungsministerium als nationaler Generalunternehmer für das Projekt Euro Hawk verantwortlich. Die Nato hat sich ebenfalls für das Überwachungssystem Euro Hawk entschieden.

Grössere Spannweite

Der Euro Hawk ist gemäss einem Sprecher von Northrop Grumman die erste internationale Version des Global Hawk, die für grosse Flughöhen und eine lange Flugdauer konzipiert worden ist. Mit einer grösseren Spannweite als ein Verkehrsflugzeug, einer Flugdauer von 30 Stunden und einer maximalen Flughöhe von knapp 20 000 Metern ist der Euro Hawk ein interoperabler, modularer und kosteneffizienter Ersatz für die veralteten bemannten Aufklärungsflugzeuge vom Typ Breguet Atlantic, die bereits seit 1972 im Dienst stehen. Der Euro Hawk ist im Übrigen das bisher grösste un-

Die Pilatus PC-21 der Luftwaffe fliegen künftig ganz in Rot

Die Schweizer Luftwaffe setzt für die Ausbildung ihrer Jetpiloten seit dem Jahr 2008 sechs Flugzeuge des Typs Pilatus PC-21 ein. Die bisherigen Erfahrungen in der Pilotenschule haben gezeigt, dass die Sichtbarkeit des rotweissen Anstrichs nicht ganz optimal ist.

Deshalb wurde beschlossen, die Pilatus-PC-21-Flugzeuge der schweizerischen Luftwaffe neu vollständig mit einer roten Bemalung zu versehen. Damit soll die Sicherheit, insbesondere im Verbandsflug unter Instrumentenflugbedingungen, noch weiter erhöht werden. Die einfarbige rote Bemalung mit einem schmalen, eleganten weissen Zierstreifen sorgt dafür, dass das Flugzeug in seinem ganzen Volumen klar erkennbar wird. Besonders positiv wird sich dies bei bewölkten Verhältnissen auswirken; dann kommt die neue rote Bemalung speziell intensiv zum Tragen, was den Fliegern beträchtlich hilft. Rot ist eine der angestammten, traditionsreichen Farben der schweizerischen Luftwaffe.

Pilatus PC-21 mit neuem Anstrich.

Kürzlich wurde die Umlackierung des ersten Flugzeugs beendet. Ein zweites Exemplar erhält den neuen Anstrich noch in diesem Herbst. Anschliessend sollen die mit dem Rüstungsprogramm 2010 geplanten zusätzlichen zwei Flugzeuge mit der roten Lackierung geliefert werden. Das Umlackieren der restlichen vier PC-21 ist für das zweite Semester 2012 vorgesehen.

Laurent Savary

bemannte Flugzeug der Welt. Die Maschine ist 14,5 Meter lang, 4,63 Meter hoch, die Flügelspannweite beträgt 39,89 Meter, das Leergewicht liegt bei knapp 7 Tonnen und das maximale Startgewicht soll über 14 Tonnen betragen.

Integrierte Lösung

Die Höchstgeschwindigkeit liegt bei 630 Stundenkilometern und wird dank einem Mantelstromtriebwerk erreicht.

Der Euro Hawk basiert auf dem amerikanischen Global Hawk in der Version RQ-4, Block 20. In Deutschland wird das Flugzeug mit einem neuen, von EADS DC entwickelten Missionssystem zur Signalaufklärung (SIGnal INTelligence – SIGINT) ausgerüstet.

Die dazugehörende Bodenstation mit Modulen für Start-, Einsatz- und Rückflugsteuerung stellt Northrop Grumman bereit. Im Rahmen einer integrierten Systemlösung liefert EADS DC darüber hinaus eine SIGINT-Bodenstation zum Empfang und zur Auswertung der vom Euro Hawk übermittelten Daten.

Pilot sitzt am Boden

Der verantwortliche Pilot sitzt beim Euro Hawk nicht im Flugzeug, sondern in der Bodenstation. Er ist über Datenfunk, direkt oder via Satellit, mit den Systemen an Bord der Drohne verbunden und kann jederzeit Änderungen beispielsweise der Flugroute oder der Flughöhe vornehmen. Der Start, die Landung und der Flugweg laufen grundsätzlich gemäss der Programmierung der Computer ab. *pj.*

Gut sichtbar ist die gewaltige Spannweite.

Cyberwar

Die Herbstveranstaltung der Schweizerischen Gesellschaft Technik und Armee (STA), die am 4. November 2010 in der Kaserne Bern stattfand, widmete sich der Internetkriminalität, die zur realen Bedrohung geworden ist.

AUS BERN BERICHTET OBERSTLT PETER JENNI

Die Melde- und Analysestelle Informationssicherung (MELANI) des Bundes hält im jüngsten Halbjahresbericht fest, dass die Spionage und der Datendiebstahl im Internet zunehmen. Immer öfter würden Webseiten oder Netzwerke benutzt, um schädliche Software zu verbreiten. Die amerikanischen Streitkräfte betrachten den Cyberspace als fünften potenziellen Kriegsschauplatz neben Boden, Luft, Meer und Weltraum.

Die Nato ihrerseits hat eine neue Abteilung «Neue Sicherheitsherausforderungen» (Emerging Security Challenges) geschaffen, die sich mit dem Terrorismus, Angriffen gegen elektronische Infrastrukturen (Cyberattacks), die Gefährdung der Energieversorgung und die Verbreitung von Massenvernichtungswaffen befassen soll.

Neue Herausforderung

Angesichts der Tatsache, dass politische, militärische und wirtschaftliche Konflikte zunehmend mit Computerviren und dem Internet ausgetragen werden, hat der Vorstand der STA beschlossen, ihre traditionelle Herbstveranstaltung dem Thema Cyberwar zu widmen.

Dies vor allem auch deshalb, weil in der Schweiz das allgemeine Bewusstsein teilweise fehlt, dass ein gut organisierter Cyberangriff ein Land auf eine Weise lahmlegen kann, wie es früher nur durch den Einmarsch einer Armee gelungen wäre. Über 200 Vertreter der Industrie, des eidgenössischen Parlaments und der Armee folgten der Einladung. Verschiedene Referenten nahmen sich dieses brisanten Themas an.

Freier Zugriff

In seinen Ausführungen führte Sandro Arcioni von der Firma Mupex Sàrl aus, dass die cyberentischen Waffen allen zugänglich seien und dass sie sich unkontrollierbar verbreiten. Weder durch eine technologische Barriere, noch finanztechnisch oder rechtmässig könne deren Verbreitung verhindert werden. Der Angreifer im Cyberspace liege immer im Vorteil. Er könne die neusten Entwicklungen zu seinen Gunsten nutzen und sei in der Lage, diese beim Attackierten zu dessen Nachteil zu verwenden. Der Betroffene müsse immer wieder reagieren und versuchen, den Angriff zu neutralisieren.

Über 200 Vertreter aus der Industrie, des eidgenössichen Parlamentes und der Armee folgten den Ausführungen zum Cyberwar in der Kaserne Bern.

Wirtschaftliche Aspekte

Die technischen und wirtschaftlichen Konsequenzen einer Attacke auf ein Unternehmen oder eine Organisation sind der Verlust der elektronischen Post (E-Mail), ein Datenverlust und die Blockierung der Informatiksysteme. Letzteres lähmt ein Unternehmen heute praktisch vollständig.

Weitere Gefahren sieht Dr. Sandro Arcioni in der Fälschung von Daten, der Hinterziehung von Zahlungsaufträgen, dem Diebstahl von Daten aller Art und dem

Definitionen

Cyberwar
«Der Cyberwar oder Informatik-Krieg wird mit dem Einsatz von Computern und Internet geführt. Er betrifft die Bereiche Politik, Zivilgesellschaft, Militär und Wirtschaft.»

Cyberspace
«Der Cyberspace besteht aus einem Netzwerk, das grenzenlos, erweiterbar und anonym ist. Die Identifikation des Angreifers ist schwierig.»

Cyberkriminalität
«Umfasst alle Gesetzeswidrigkeiten, mit denen ein Informatik-System, das an ein Netz angeschlossen ist, geschädigt wird.»

Lahmlegen der Verkaufs- und Produktionsaktivitäten.

Aktuelle Bedrohungslage

Marc Henauer, Chef der Sektion Cybercrime (MELANI) beim VBS, wies in seinen Darlegungen auf die Risiken und die Bedrohung der Schweiz hin. Mit der Zunahme der Bedeutung der Informationstechnologie für Geschäftsprozesse und Finanztransaktionen sowie der steigenden Zahl von Teilnehmern an diesen Prozessen steige auch die Möglichkeit für Betrug, Spionage, Erpressung und Sabotage. In jüngster Zeit wurden neue Akteure wie Staaten und das organisierte Verbrechen als Störenfriede festgestellt.

Ebenfalls verändert hätten sich die Methoden und Motive der Akteure. Sie suchten kommerziellen Gewinn, Wissenstransfer und hätten politische Motive. So wurde im Herbst 2009 ein gezielter Hackerangriff auf das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) ausgeführt. Solche Attacken würden in der Regel nicht von einzelnen Akteuren ausgeführt, sondern beispielsweise von Staaten, die über ausreichende finanzielle und personelle Ressourcen verfügen. Experten schätzen, dass zum Beispiel der Angriff auf iranische Installationen im vergangenen Herbst mit STUXNET mehrere Millionen Franken erfordert hat.

Henauer wies weiter darauf hin, dass ein wachsender Untergrundmarkt für das Aufspüren von Sicherheitslücken und das verbreiten von schädlicher Software existiere. Entsprechende Werkzeuge und Leistungen könnten eingekauft werden. Zur Typologie der Angreifer unterschied der Referent folgende Akteure: Hobby-Hacker, Hacker, Experten und Spezialisten.

Heute genüge nach Marc Henauer zur Abwehr einer Attacke das Installieren einer Antivirensoftware oder die Aufdatierung eines Betriebssytems und einer Applikation nicht mehr, auch ein geschlossenes, lokales Netzwerk reiche nicht mehr aus.

Gewisse Viren seien in der Lage, derartige Sperren zu überspringen. Grundsätzlich gebe es eine 100-prozentige Sicherheit ohnehin nicht. Es gelte, die vorhandenen Risiken zu verringern und die Sicherheit zu optimieren. Eine nicht unerhebliche Folge seien steigende Kosten für verbesserte IT-Lösungen und zusätzliche physische und personelle Aufwendungen. All dies führe zu Einbussen in der Effizienz.

Bester Schutz

Schliesslich wies der Referent doch noch auf einen positiven Aspekt hin. Die Informationstechnologie sei «immer dieselbe» und so verhielte es sich mit den Angriffen, egal welcher Art die Absichten seien. Den besten Schutz vor Attacken böten in die Tiefe gehende, integrale Sicherungsprozesse.

In eine ähnliche Richtung äusserte sich der Vertreter der Firma Elca Informatik AG, Marco Ferro. Gemeinsam mit dem Kunden wird eine sorgfältige Analyse der vorhandenen IT-Systeme gemacht. Nach der Erhebung des Ist-Zustandes werden die Wünsche und Bedürfnisse des Kunden erfasst. Jetzt gilt es abzuwägen, welcher Teil des IT-Systems besonders gefährdet ist und somit verstärkt geschützt werden muss. Nur mit einem systematischen Vorgehen können die notwendigen Massnahmen gemeinsam festgestellt und anschliessend realisiert werden.

Hans Jürg Wieser, Vorstandsmitglied der STA, erläuterte engagiert die Gefahren bei der Stromversorgung grosser Agglomerationen.

Kritische Infrastrukturen

Am Beispiel der Energieversorgung wies Hans Jürg Wieser, Vorstandsmitglied der STA, auf die Gefahren in modernen Agglomerationen hin. Gerade in der Stromversorgung ergäben sich immer mehr Steuerungsprozesse. Alles hänge vom Strom ab: die Wasserversorgung, das öffentliche Transportwesen, die industriellen Anlagen, öffentliche und private Gebäude, die Finanzwelt.

Im Bereich der Stromversorgung zeichne sich ein Wechsel von der statischen Infrastruktur zur dynamischen ab. Ausgelöst werde dieser Wechsel durch die starke Nachfrage, die erneuerbaren Energien und die neu entstehenden «Riesenstädte». Weiter komme hinzu die Liberalisierung der Strommärkte, welche unterschiedlichste Interessen der Produzenten und Konsumenten auslöse.

In besonderen Fällen ist der Konsument gleichzeitig Produzent. Am Beispiel des Besitzers einer Photovoltaikanlage lasse sich das erläutern: Der Besitzer speist den überschüssigen Strom seiner Anlage in das öffentliche Stromnetz ein, von dort bezieht er Energie, wenn die Sonne einige Tage nicht scheint.

Hans Jürg Wieser wies darauf hin, dass ohne die zur Steuerung dieser Prozesse notwendigen Informations- und Kommunikationstechnologien diese Herausforderung nicht zu bewältigen sei. Diese Infrastrukturen müssten aber ebenfalls gegen Cyberattacken geschützt werden. Solche Herausforderungen gelte es zu bewältigen.

Boshafte Software

Virus: sich duplizierendes Programm auf anderen Computern
Worm: nutzt die Ressourcen eines Computers aus, um sich zu reproduzieren
Wabbit: Programme, die sich selber antworten (kein Virus, kein Worm)
Trojan: führt schädliche Abläufe ein ohne Einwilligung des Nutzers
Backdoor: öffnet den betrügerischen Zugang zu einem System
Spyware: sammelt ohne Erlaubnis Informationen auf einem Computer und leitet diese an Dritte weiter
Keylogger: speichert unerkannt die Tastenanschläge des Nutzers
Exploit: Programm, das eine Schwachstelle einer Software ausnützt

Stromausfall in Brasilien

Am 11. November 2009 gab es in Brasilien einen weitreichenden Stromausfall mit Folgen.

Sao Paulo und Rio de Janeiro blieben stundenlang ohne Strom. Auch in Paraguay fiel kurzzeitig der Strom aus. Zehntausende Menschen sassen in Aufzügen und in der U-Bahn fest. Die Evakuierung war schwierig, weil das Telefonsystem wegen Überlastung zusammenbrach.

Auch das Mobiltelefonnetz kam komplett zum Erliegen. Über die Ursache des Ausfalls gab es Spekulationen. Als mögliche Ursache wurde ein Hackerangriff ins Feld geführt. (Halbjahresbericht 2010, MELANI)