„Bedrohungen im Cyber-Raum – praktische Umsetzung der Cyber Awareness in einer Kommandobehörde der Luftwaffe"

Das Dezernat „A 6 e – CyberAwareness/IT-Sicherheit" des Zentrum Luftoperationen (ZentrLuftOp) stellt sich den Bedrohungen im Cyber-Raum

Oberleutnant Marcus Mengs, IT-Sicherheitsoffizier im Zentrum Luftoperationen der Luftwaffe

Die Auswirkung der Erfindung von Rechnernetzen, der Etablierung des Internets und die allgemeine Computerisierung haben eine digitale Revolution ausgelöst, die sich zunehmend auf viele Lebensbereiche auswirkt. Gesellschaft, Staat und Wirtschaft sind auf Informationen und Daten aus einem global vernetzten Milieu, dem sogenannten Cyber-Raum, angewiesen.
„Der Cyber-Raum ist der virtuelle Raum aller auf Datenebene vernetzten IT-Systeme im globalen Maßstab. Dem Cyber-Raum liegt als universelles und öffentlich zugängliches Verbindungs- und Transportnetz das Internet zugrunde, welches durch beliebige andere Datennetze ergänzt und erweitert werden kann."

Die vorstehende Begriffsdefinition entstammt der „Cyber-Sicherheitsstrategie für Deutschland" des Bundesministerium des Inneren. Seit der Entdeckung des hochentwickelten Computerwurmes StuxNet im Jahre 2010, welcher mutmaßlich das iranische Atomprogramm zum Ziel hatte, haben sich Begriffe wie „Cyber-War" und „der digitale Erstschlag" etabliert. Bedrohungen für die reale Welt aus dem Cyber-Raum heraus wurden durch die Veröffentlichungen Edward Snowdens für die breite Öffentlichkeit greifbar. Man vermutet, dass StuxNet 2007 von mehreren Staaten mit Kosten von geschätzten 50 Millionen US-Dollar (© http://www.sz-online.de/nachrichten/kultur/die-unsichtbare-bedrohung-3012499.html) erstellt wurde. Inzwischen hat sich eine Situation entwickelt, die es einem einzelnen verärgerten Konsolenspieler erlaubt, ein Botnetz (Eine Gruppe von mit Schadsoftware infizierten, vernetzten Geräten unter Kontrolle eines Angreifers) anzumieten und damit sogar gut aufgestellte Internetdienste wie Twitter, Netflix und Ebay für Stunden weltweit zum Erliegen zu bringen (© http://www.wsj.com/articles/october-internet-attack-targeted-playstation-network-researchers-say-1479250847). Ein solches Botnetz bestand vor einigen Jahren nur aus Computern. Die jüngsten Angriffe erreichen bisher ungesehene Dimensionen und gehen von Smart-TVs, Kameras, Kühlschränken, Waschmaschinen und Glühbirnen aus. Diese Geräte gehören zum „Internet der Dinge", sind global vernetzt und finden mittlerweile ihren Platz in zahlreichen Haushalten.
Allein dieser kurze Abriss zeigt, dass sich die heutige Bedrohungslage aufgrund der Vielfalt der Akteure, der technischen Komplexität und der globalen Dislozierung nicht in wenigen Worten beschreiben lässt. Missbrauchspotenziale durch nicht gewollte Eingriffe und Attacken Dritter steigen signifikant. Wir leben in Zeiten, in denen sich jeder Interessierte für 5 US-Dollar Hardware beschaffen kann, die geeignet ist, geschützte Computernetze ohne technisches Fachwissen empfindlich zu stören. Ein jüngeres Beispiel ist die öffentliche Bereitstellung von Anleitungen, Software und Videos zur Herstellung eines dieser Werkzeuge, zusammengefasst unter dem einprägsamen Marketingnamen „PoisonTap".
Es besteht die Notwendigkeit, sich vor den angedeuteten Bedrohungen zu schützen. Hierbei kommt nicht nur die Schutzbedürftigkeit von Informationen unter militärischen Gesichtspunkten zum Tragen, auch das Grundbedürfnis nach Sicherheit und das Grundrecht auf informationelle Selbstbestimmung sind durch die aktuelle Bedrohungslage betroffen. Die Verfügbarkeit, der Schutz und die Unverfälschtheit von gespeicherten, übertragenen und verarbeiteten Informationen und Daten sind folglich von vitalem Interesse.

Das Dezernat
„A 6 e – CyberAwareness/IT-Sicherheit"
Mit dem Dezernat „A 6 e – CyberAwareness/IT-Sicherheit", steht dem Zentrum Luftoperationen eine Teileinheit zur Verfügung, welche genau an dieser Problemstellung ansetzt. Zum Betätigungsfeld gehört die „klassische" IT-Sicherheit, welche etablierte technische, organisatorische und personelle Mittel nutzt, um die tatsächliche Gefährdung auf ein Mindestmaß zu reduzieren – dennoch verbleibt hier oft ein Restrisiko.
Betrachtet man tatsächliche Cyberattacken in ihrer ganzen Täterbandbreite und Durchführungskomplexität, angefangen von „Spielereien durch Möchtegernhacker" (Script-Kiddies) ohne konkretes Ziel, über die in Untergrundnetzwerken (Darknet) agierende organisierte Kriminalität, bis hin zu „fortgeschrittenen, andauernden Bedrohungen" (Advanced Persistent Threats, APT) durch meist staatliche Akteure wie Nachrichtendienste, haben die meisten Szenarien nach wie vor eine Gemeinsamkeit:
Abseits aller Technik ist der Erfolgsgarant für Cyberangriffe die Ausnutzung der Schwachstelle MENSCH.

Genau diesen Fakt greift das Betätigungsfeld „CyberAwareness" auf und stellt den Anwender von IT-Systemen in den Fokus. Erklärtes Ziel ist die Schaffung des nötigen Gefahrenbewusstseins, um den sicheren Umgang mit digitalen Medien für jeden IT-Nutzer des Kommandobereichs zu ermöglichen. Hierdurch wird die potentielle

Grafik: Fraunhofer-Gesellschaft

„Schwachstelle Mensch“ in ein weiteres Hindernis für Angreifer verwandelt.

Die weitaus größte Herausforderung hierbei ist die Heterogenität der Zielgruppe für CyberAwareness-Ausbildungen. Die Bandbreite bewegt sich von der jungen Soldatin, die digitale Medien ganz selbstverständlich einsetzt, die über ein Smartphone permanent weltweit kommuniziert und große Teile des sozialen Alltags online bestreitet, bis zum nicht computeraffinen, lebensälteren Bundeswehrangehörigen. Dem begegnet das Dezernat mit einem ebenso breitbandig aufgestellten Personalkörper. Angefangen vom IT-Sicherheitsbeauftragten mit mehreren Jahrzenten nationaler und internationaler Erfahrung, über „WhiteHat-Hacker“ mit praktischer Erfahrung und Kenntnissen im Ausnutzen technischer Schwachstellen, bis hin zum jungen, gelernten Anwendungsprogrammierer ist Expertise vertreten.

Der Digitalisierung kann sich mittlerweile niemand mehr entziehen und damit ist jeder den beschriebenen Gefahren ausgesetzt. Dass sich dennoch nicht jeder dieses Umstandes bewusst ist, stellt die zweite große Herausforderung dar:

die Schaffung dieses Bewusstseins oder eben dieser „Awareness“.

Die breite Betroffenheit wird durch einen ebenso breiten thematischen Ansatz vermittelt. Auch wird das private Umfeld aufgegriffen, in welchem „digitale Sorglosigkeit“ beginnt, bevor sie sich im Arbeitsumfeld auswirkt. Mit Live-Hackings um Themen wie „Unsichere WLAN Netze“ oder „Wenn USB zum Feind wird!“, wurden Gefahren am praktischen Beispiel veranschaulicht, aber auch konkrete Handreichungen zur Selbsthilfe gegeben. Für weniger Technikaffine wurden „Chancen und Gefahren des Internets für Kinder und Jugendliche“ unzensiert dargestellt. Insbesondere Soldaten und Mitarbeitern mit Kindern oder Enkeln wurde hier spürbar bewusst: der Gedanke, von digitalen Bedrohungen nicht (mehr) betroffen zu sein, ist ein gefährlichen Irrtum. Unachtsamer Umgang mit modernen Medien durch Kinder und Jugendliche kann für Erziehungsberechtigte schnell strafrechtliche Konsequenzen nach sich ziehen.

Die letzten Zweifel an der Relevanz und Tragweite des gesamten Themengebietes, konnten im Vortrag „Cybercrime: Trends, Bedrohungssituation“ des Landeskriminalamtes NRW ausgeräumt werden.

Die dritte Herausforderung liegt in der Gewährleistung der Themenaktualität. Das Bestreben des Dezernates „IT-Sicherheit / CyberAwareness“ ist es, Trends zu verfolgen, tatsächliche Bedrohungen herauszufiltern und nutzergerecht aufzubereiten. Genutzt werden hierfür zum einen Publikationen, wie zuletzt zu „Pokémon Go“ (Smartphone App, welche Spiel und Realität verknüpft und zu erheblichen Datenschutz- und Sicherheitsbedenken führte), welche schnell eine breite Leserschaft über die Dienststellengrenzen hinaus erreichen. Zum anderen wird eine hohe Aktualität durch den ständigen Informationsaustausch mit Fachkreisen, Behörden und Firmen der IT-Branche erreicht.

Nach einem guten Jahr mit regelmäßig durchgeführten CyberAwareness-Maßnahmen im Zentrum Luftoperationen stellt sich die Frage nach deren Erfolg. Trotz steigender Zahlen an Angriffsversuchen durch Spammails und schadhafte Webseiten, bleibt die Zahl der IT-Sicherheitsvorkommnisse konstant niedrig. Das Rückfragevolumen zu ebensolchen Mails und Webseiten nimmt aufgrund erhöhter Nutzersensibilisierung dagegen deutlich zu! Laien berichteten, dass sie mit Hilfe von Handouts aus dem Bereich CyberAwareness in der Lage waren, selbstständig verschlüsselte Internetverbindungen aus Einsatzgebieten in die Heimat aufzubauen. Weitere Organisationsbereiche haben erstellte CyberAwareness-Publikationen angefragt, weil Informationen mündlich weitergegeben wurden – die Themen bleiben also im Gespräch und damit in den Köpfen. Zusammenfassend fällt die Antwort auf die Frage nach dem Erfolg der Maßnahmen also nicht nur positiv aus, die Anfangserwartungen wurden jedoch übertroffen.