Fotos: Bundeswehr/Tom Twardy (5)

Anspruchsvoll: Oberstleutnant Thorsten Bartel, Leiter des deutschen Abwehr-Teams, erklärt den Teilnehmern die Netz- und Systeminfrastuktur (l.). Deren Aufgabe ist es, in der Kommandozentrale in Euskirchen Cyberangriffe abzuwehren (o.m. u. o.r.). Infiltrierte Systeme, die durch Cyber-Angriffe ausgeschaltet worden sind, erscheinen rot (u.r.), nicht-infizierte Systeme sind grün dargestellt (u.m.).

Der Angriff

Cyber-Attacken geschehen täglich – und können verheerenden Schaden anrichten. Die NATO-Übung „Locked Shield“ gibt Einblicke. aktuell war in Euskirchen mit vor Ort.

Von Tilman Engel
Fotos Tom Twardy

Das Szenario

Geübt wurde in einem extra aufgebauten, abgeschlossenen Netzwerk und anhand eines fiktiven Szenarios: Nach einem digitalen Angriff auf die IT-Systeme eines Landes ist die IT-Infrastruktur in ihrer Funktion stark beeinträchtigt. In der Übung hat das deutsche Rapid Reaction Team (genannt „Blue Team 04“) den Auftrag, die rund 70 Systeme der digitalen Infrastruktur und die wichtigsten industriellen Kontrollsysteme gegen eine Vielzahl von Cyber-Angriffen zu schützen. Zentrale Aufgabe ist, die andauernde Verfügbarkeit aller Systeme zu erhalten. Auch die Kontrolle über eine Aufklärungsdrohne, die offenbar per Cyber-Attacke gekapert werden soll, muss gesichert bleiben.

Der Verlauf

Aus dem Lagebericht: „Blue Team 04 ist seit mehreren Stunden Cyber-Attacken ausgesetzt. Die Anzahl der Angriffe nimmt fortwährend zu. Das Handeln von Script Kiddies (Cyber-Amateure) kann aufgrund der Qualität der Angriffe ausgeschlossen werden. Die Herkunft der Angriffe ist unklar, sie erfolgen aber vermutlich in fremden Auftrag. Es gelang den Angreifern erneut, die meisten der eigenen Webseiten durch Defacements oder Veränderungen an den Datenbanken zu übernehmen. Es sind permanent Maßnahmen notwendig, um die Kontrolle über die Drohne zu halten. Um 1205 Zulu wurde wieder eine relevante Sicherheitslücke in der Mission Control (Steuerung) der Drohne entdeckt. Blue Team 04 hat die Kontrolle über wesentliche Komponenten wieder hergestellt.“ „Wir haben zum Teil einfach nur noch auf die Tastatur gehauen, weil das System so langsam war und unsere Gegenmaßnahmen einfach nicht schnell genug umsetzte, um wirksam zu sein“, sagt einer der deutschen IT-Experten. Der administrative Zugang zum Netzwerk-Router wird zeitweise verloren. Da das virtuelle Netzwerk zeitweise nur sehr langsam arbeitet, greifen die Gegenmaßnahmen des Teams nur verhalten.

„Uns ist dann wirklich das Herz in die Hose gerutscht, weil wir fast den Zugang zum Router verloren haben. Bei den ersten Angriffen war es tierisch aufregend.“

Mehrfach wird die Aufklärungsdrohne durch den Cyber-Angreifer übernommen und in den Luftraum des Nachbarlandes gesteuert. Es gelingt dem deutschen Expertenteam jedoch jedes Mal, die Kontrolle zurückzugewinnen und die Drohne rechtzeitig vor einem Absturz auf Gegenkurs zu bringen. Dennoch kommen fast alle digitalen Angriffe durch die digitalen Sicherungen des Übungs-Netzwerkes durch.

Parallel zu den Cyber-Angriffen spielt die fehlgeleitete Drohne eine wichtige Rolle im politischen Konflikt zwischen beiden Staaten. Im Übungsszenario nutzen die Konflikttreiber eine überzeichnete Drohnengefahr als Beweis für die aggressiven Absichten der Gegenseite.

Oberleutnant Cerderberg: „Es war ein riesiges Erfolgserlebnis, als wir die Kontrolle über die Drohne wieder zurück gewonnen haben. Auch wenn diese danach gleich wieder verloren ging.“

Bekannte Cyber-Angriffe

- 2007 wurden in Estland die Online-Auftritte der öffentlichen Verwaltung lahm gelegt. Als eine Folge dieser Angriffe etablierte die estnische Regierung den Aufbau des NATO Cooperative Cyber Defence Center of Excellence (CCDCOE) in Tallinn.
- Im Frühjahr 2015 gelang es Anhängern der Radikal-Islamisten von Daesh, die Programme des französischen Senders TV 5 zu infiltrieren und eigene Propaganda-Videos zu übertragen.
- VISA und Master Card wurden 2012 Opfer eines Spähangriffes, bei dem Daten von zehn Millionen Kunden gestohlen wurden.
- Mit dem Virus Roter Oktober, der 2012 entdeckt wurde, sind jahrelang weltweit Daten in einer großen Bandbreite abgeschöpft worden.
- Der Stuxnet-Virus griff ab 2009 weltweit industrielle Kontrollsystemen an. Experten gehen heute davon aus, dass er gezielt das iranische Atomprogramm angreifen sollte.
- Im Mai 2015 wurde von Servern des Bundestages ein Datenabfluss mit unbestimmter Zielrichtung festgestellt. Über sechs Monate hatten die Angreifer den Virus in mehreren, unverdächtigen Segmenten auf den Servern des Bundestages installiert.
- Im März dieses Jahres kam es zu zahlreichen virtuellen Angriffen auf Krankenhäuser in Europa und den USA, bei denen der Zugang zu Patienten und Operationsdaten gesperrt wurde.

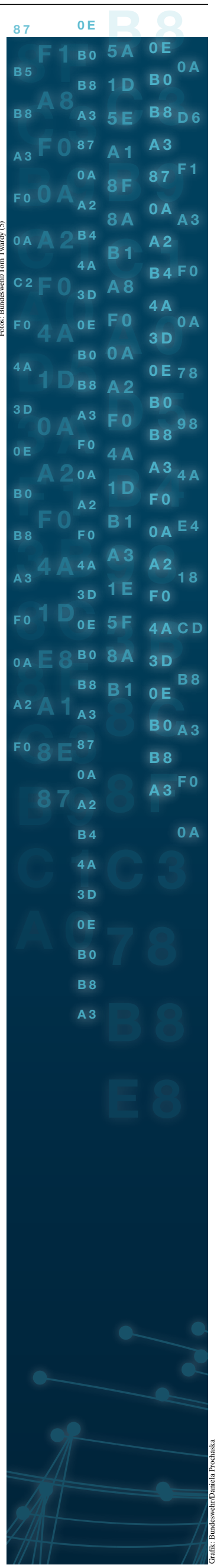
Das Fazit

Blue Team 04 es gelang es, die Verfügbarkeit der IT-Infrastruktur weitgehend aufrechtzuerhalten. Die Forensiker im Team konnten Schadsoftware identifizieren und einem Drittstaat zuordnen. Eine unzureichende Überwachung der Systeme führte jedoch zu einer hohen Anzahl erfolgreicher Cyber-Angriffe. Nachdem der Angreifer 60 Prozent aller Systeme ausgeschaltet hatte und so den Verteidigern die Möglichkeiten genommen war, ihren Auftrag weiter zu verfolgen, wurde die Übung beendet.

„Eigentlich war ich während der ganzen Übung relativ emotionslos, aber ich hatte nicht mit so vielen Angriffen gerechnet“, fasst Oberstleutnant Thorsten Bartel, der Leiter des deutschen Teams, zusammen. „Eigentlich würde niemand in der echten Welt versuchen, so ein verseuchtes System noch zu retten, sondern dies stattdessen vollständig neu aufsetzen.“

Die Verteidigung

Beim Ausfall eines Systems ermittelt die Cyber-Abwehr zunächst die zerstörte oder verseuchte Datei. Diese wird dann aus dem Backup heraus wieder hergestellt. Dann ist es die nächste Herausforderung, diese Befehlsdatei über den ebenfalls infizierten Server wieder der fehlgeleiteten Drohne zu übermitteln. Wird der eigentliche Virus jedoch nicht erkannt, und somit auch keine Sicherung dagegen vorgenommen, kann der Angreifer über Systemlücken, diese Schadsoftware immer wieder neu aktivieren.



Grafik: Bundeswehr/Daniela Prochaska