1. Ablichtung, 36 Seiten gh.

GEHEIM

- amtlich geheimgehalten -

42

GEHEIM

GUTACHTEN

zu Strafsache gegen KLAG

AZ: 3 StE 1/13-2

1 Mehrfertigung
1 DVD-GA

Sachverständiger: Dr. Sandro Gaycken, Institut für Informatik, Freie Universität Berlin. Experte für Cyber Warfare, Cyber Defense, Cyber Spionage und allgemein Cyber Security.

Anschrift: Dr. Sandro Gaycken, Institut für Informatik, FU Berlin, Fabeckstraße 15, 14195 Berlin

Zuständige Kammer / Auftraggeber: Oberlandesgericht Koblenz, Staatsschutzsenat, Stresemannstraße 1, 56068 Koblenz

Datum der Abfassung: 29.8.2013

Beschreibung und Umfang: Dieses Gutachten beschreibt Schäden, die durch Cyberangriffe auf der Basis einiger durch KLAG möglicherweise offengelegter Informationen zu IT-Strukturen entstehen könnten, und es beantwortet einige Fragen des Angeklagten zum Sicherheitsstand der betroffenen IT-Strukturen. Der Umfang beträgt 36 Seiten.

Verwertete Unterlagen: Es wurden die Bände 21 bis 24 der überlassenen Gerichtsakten verwertet.

43

Aufbau:

1. Überblick zur taktisch-strategischen Nutzbarkeit der betroffenen Informationen

2. Konkrete Anmerkungen zu einzelnen Punkten der betroffenen Informationen

3. Schäden für die NATO

4. Antworten auf die gestellten Fragen

5. Zusammenfassung

1. Überblick zur taktisch-strategischen Nutzbarkeit der betroffenen Informationen

Da Cyber Warfare und Cyber Spionage komplexe und zum Teil noch junge Phänomene sind, wird das Gutachten mit einem Gesamtüberblick beginnen. Dabei werden auf der Basis der durch die betroffenen Informationen generierten Kenntnis der betroffenen Systeme prinzipiell ermöglichte Aktivitäten in ihrem taktischen Vorgehen und in ihrer strategischen Bedeutung geschildert.

1.1 Zwei Basisvarianten von Nutzungen

Die offengelegten Informationen können grundlegend in zwei Weisen von Angreifern genutzt werden.

1.1.1 Einfache und äußere Störung

Die erste Variante der Nutzung besteht in einer einfachen Störung der Strukturen. Dies ist besonders gut möglich, wenn die Abhängigkeitsverhältnisse der Server untereinander und die technischen Adressen und Details zu den darauf laufenden Diensten (ansprechbare Software) bekannt sind. In diesen Fällen lassen sich ressourcenerschöpfende Angriffe wie die bekannten Denial of Service-Angriffe ausführen. Bei solchen Angriffen werden bestimmte Dienste im Rahmen der Serverstruktur mit massenhaften oder schlecht verarbeitbaren Daten kontaktiert, so dass diese Dienste einen Großteil der Rechenkraft und der Bandbreite für diese Anfragen verwenden müssen und so legitime Anfragen und andere Dienste nicht länger möglich sind. Zudem ist es möglich, bei schlecht gewählten Abhängigkeitsverhältnissen der Server zueinander, weitere Teile der Netzwerke lahmzulegen, indem man zentrale Server zu einem Ausfall bringt.[1]

Im vorliegenden Fall wäre es denkbar, dass selbst ein weniger talentierter Angreifer Störungsangriffe in das NS-Netzwerk einbringen kann, der dann die Funktionen der Server leicht und temporär bis massiv und dauerhaft beeinträchtigt. Da die Abhängigkeit einiger Funktionen wie etwa des Integrated Command & Control (ICC) von einem reibungslosen Betrieb in Echtzeit sehr hoch und im Missionsfall missionskritisch ist, können solche Störungen bereits erheblich operative Beeinträchtigungen und damit Gefährdungen für Leib und Leben produzieren.

1.1.2 Zugang

---

[1] Derartige Störungen sind immer wieder zu beobachten, wie etwa bei den bekannten Vorfällen in Estland 2007 oder bei Angriffen auf US-Banken 2012.

Die zweite Variante der Nutzung besteht im Zugang zu den Strukturen. Diese Variante ist anders, da im Falle der Störung kein Zugriff auf eine Administrationsebene eines Rechners stattfinden muss. Bei einer Störung finden Angriffe nur äußerlich, auf der Ebene legitimer Außenanfragen statt. Bei einem Zugang dagegen kann ein Angreifer auf verschiedenen Ebenen im System auf das System zugreifen und abhängig von den mit der Ebene und der Art des Zugriffs verbundenen Rechten direkt und mit den Handlungsoptionen eines legitimen Users im Zielsystem agieren. So wird das Handlungsspektrum gegenüber der einfachen Störung um ein Vielfaches erweitert.

Zugang kann auf verschiedene Weise hergestellt werden, wobei drei Varianten für den vorliegenden Fall besonders relevant sind:

- über Passwörter, die einen direkten Zugang auf verschiedene Systemebenen mit unterschiedlichen weiteren Zugriffstiefen ermöglichen, abhängig von den mit dem Zugang verbundenen Privilegien. Damit zusammenhängend gibt es auch einen Zugang über eine sogenannte Eskalation von Privilegien, wobei nach einem bereits gelegten Zugang versucht wird, auf eine Ebene mit weiter ausgreifenden Privilegien zuzugreifen, so dass eine größere Zugriffstiefe möglich wird,

- über laterale Bewegung, wobei ein in einem Teilsystem befindlicher Angreifer durch Schwächen der Netzwerk- und Sicherheitsarchitektur auf andere Teile des Systems zugreifen und sich so innerhalb des Systems weiterbewegen kann,

- über Verwundbarkeiten in den Systemen auf Hardware-Ebene oder auf Software-Ebene, wobei auch ohne eine Nutzung von Passwörtern durch kritische Schwächen in Hard- und Software auf die Systeme zugegriffen werden kann.

Diese Punkte sollen gleich näher ausgeführt werden.

Zunächst muss aber das Caveat vorgebracht werden, dass im vorliegenden Fall diese Zugangsweisen auf die inneren Strukturen der NS-Systeme erst ermöglicht sind, wenn sich ein Angreifer prinzipiell Zugriff auf das NS-System verschaffen kann. Dies ist allerdings nicht übermäßig schwer und wird durch die von dem KLAG verfügbar gemachten Informationen erleichtert. Ein Angreifer kann, um in das NS-System einzudringen:

- einen weiteren Innentäter anheuern, nach einigen Informationen von KLAG wie Email-Adressen und Serverzuständigkeiten sogar gezielt nach bestimmten Zugriffsrechten. Dabei ist anzumerken, dass das NATO SECRET System aufgrund des Paradigmas "Responsibility To Share" eine ungewöhnliche große

Ausweitung aufweist, wobei nicht nur die Ausweitung HQ Ramstein, sondern das gesamte NS-Netzwerk gemeint ist. Der Zeuge MULQUEEN gibt diese Ausweitung mit bis zu 65.000 Nutzern an. Es ist anhand der Unterlagen und Aussagen nicht bekannt, ob es zuverlässige Trennungen und Sicherheitsmaßnahmen zwischen dem großen NS-Netzwerk und dem HQ Ramstein NS-Netzwerk gibt. Allerdings gibt es auf jeden Fall physische Verbindungen zwischen den Netzwerken (um die C&C-Kommunikation zu ermöglichen, die Kommunikation und den Tabellenaustausch mit den CAOCs und weitere Applikationen wie JChat. Bei NS NIRIS Extern und NS NIRIS Intern ist hier auch zum Beispiel direkt erkennbar, dass es sich lediglich um zwei virtuelle Netzwerke handelt, die auf einem physischen Netzwerk laufen), so dass prinzipiell eine Reihe von Übergängen existiert. Diese Übergänge können prinzipiell durch die offengelegten Informationen genutzt werden, um von jedem Punkt des NS-Netzwerkes auf die betroffenen Systeme zu gelangen. Die entsprechenden Server könnten etwa direkt an ihren Adressen mit den Passwörtern angesprochen werden. Diese hohe Ausdehnung des NS-Systems ist problematisch, da insbesondere bei einem professionellen Nachrichtendienst wie dem russischen oder dem chinesischen davon auszugehen ist, dass bereits Innentäter in diesem großen Netzwerk agieren. Diese Innentäter können dann über die bereitgestellten Informationen Zugriff auf die entsprechenden Server erhalten,

- über die Zulieferer fingierte Hardware und Software einschleusen, was ein gängiges Vorgehen nachrichtendienstlicher Angreifer darstellt,[2] wobei die von KLAG offengelegten Informationen zumindest Indizien über potentielle Zulieferer liefern, da die im Rahmen der NATO-Strukturen vorhandenen Produkte nur über bestimmte Zulieferer geliefert und gewartet werden können. Hier ist zudem denkbar, dass Herr KLAG über seine Tätigkeit als Service Level Manager entsprechende Informationen mündlich nachliefern könnte, was aber spekulativ ist,

- fingierte PDF- oder OpenOffice-Dokumente über das PAN-System an legitime Empfänger im NS-Netzwerk schicken, zu scheinbar legitimen Prozesse (siehe unten: Spearphishing), wobei KLAG offengelegt hat, dass Adobe Acrobat und OpenOffice installiert sind, die für diese dokumentbasierten Angriffe entsprechende Angriffsvektoren bieten und wobei KLAG die Email-Adressen für das Versenden solcher Angriffe zur Verfügung gestellt hat,[3]

---

[2] Derartige, sogenannten "Supply Chain"-Angriffe wurden vermutlich bei Stuxnet genutzt und sind Gegenstand verschiedener politischer und wissenschaftlicher Beschäftigungen.

[3] Derart fingierte Word-Dokumente und PDFs wurden etwa häufig bei vermeintlich chinesischer Industriespionage wie im Fall GhostRat genutzt.

- versuchen, Wechselmedien einzuschleusen.

Ist die Hürde zwischen dem PAN- und dem NS-Netzwerk einmal übersprungen, kann der Angreifer aufgrund der offengelegten Informationen auf die entsprechenden Server zugreifen und die oben erwähnten Angriffsvektoren im NS-System nutzen, um tiefer in dessen Strukturen einzudringen, was nun genauer ausgeführt werden kann:

- Zum einem Systemzugang über Passwörter: Der Angreifer kann über die Passwörter auf jede beliebige Systemebene zugreifen, wobei insbesondere die Root-Passwörter einen verheerend weiten und tiefen Systemzugriff erlauben. Ein Zugriff über Root erlaubt einem Angreifer jede Art von Aktivität im Zielsystem wie das Anlegen weiterer Nutzer und Hintertüren, die Modifikation bestehender Software und bestehender Daten und Datenströme und die Installation schadhafter Software. Daher macht diese Zugang es auch besonders schwer, einen Angreifer zu entdecken und ermöglicht es dem Angreifer oft, für sehr lange Zeit unentdeckt zu agieren. Teilweise können über Root angehende Angreifer auch nur schlecht wieder aus den Systemen entfernt werden. Hierbei ist außerdem anzumerken, dass das NATO Security Script, das ein Zugang auf Root-Ebene verhindern soll, möglicherweise Schwächen aufzeigt und außerdem bei einigen operativen Systemen nicht eingeschaltet war. Schwächen könnten sein, dass das Script selbst angreifbar ist oder dass ein Root-Zugang nur für den echten Reboot vor Ort verhindert wird, nicht aber für Root-Zugänge, die im laufenden Betrieb durch etwa das Öffnen einer neuen Shell ermöglicht werden. Es gilt aber ohnehin, dass miteinander verbundene Systeme immer nur so sicher sind wie ihr schwächstes Glied. Ist das NATO Security Script also an einem System nicht eingeschaltet, das aber mit den anderen Systemen verbunden ist, so kann ein Angreifer über den Root-Zugang auf diesem einen System zwar nicht direkt einen Root-Zugang bei den anderen Systemen erreichen (sofern die eben genannte Option ausgeschlossen werden kann), er kann aber alle möglichen Angriffe im Netzwerk über das infiltrierte System laufen lassen, was mitunter ausreichend ist, da er in dem befallenen System die höchsten Rechte und Privilegien wahrnehmen kann. So ist auf diesem Wege auch eine Eskalation von Privilegien möglich, indem ein Angreifer etwa in einem infizierten System - sofern dieses dazu tauglich ist - einen Administrator mit hohen Rechten für weitere Systeme anlegt, was folgend den weiteren Systemen mitgeteilt wird, die folgend entsprechend offen sind.

- Zu einem Systemzugang über laterale Bewegung: Ein Angreifer kann auf Basis der von KLAG bereitgestellten Informationen auch laterale Bewegungen in den Systemen vornehmen, indem er etwa ein infiziertes System als "Beachhead" nutzt, um von dort aus angeknüpfte Systeme mit eingebrachter Schadsoftware von Innen anzugreifen oder indem er sich durch einen hoch privilegierten Zugang und

durch eine Kenntnis des Zielsystems quer durch das Netzwerk des Zielsystems bewegen kann und so von einem Server auf viele andere zugreifen kann. Dies ist durch die offengelegten Informationen möglich, was eines der größten Probleme für die NATO in Folge des Vorfalls generiert, da sich ein Angreifer mit den Informationen des KLAG bei Zugang auf das NS-System Zugang zu den betroffenen Strukturen verschafft haben, um dann von dort aus lateral weiter in das NS-System vorzudringen, so dass inzwischen eben nicht nur die Serverstruktur des HQ Ramstein, sondern das gesamte NS-Netz infiziert sein könnte. Dieser Punkt soll später noch genauer ausgeführt werden.

- Zu einem Systemzugang über verwundbare Hard- und Software: Schließlich ist einem Angreifer auch der Zugang über verwundbare Hardware und Software durch KLAG ermöglicht. Auch dieser Punkt ist besonders fatal, da hier auch unabhängig von Passwörtern oder von den möglicherweise erfolgten Passwortänderungen noch Zugänge durch Verwundbarkeiten geschaffen werden können, die dem Opfer nicht bekannt sein müssen und die nur durch ein vollständiges Replacement der Strukturen im gesamten NS-System behoben werden können. Im vorliegenden Fall wird etwa offenbart, dass die NATO im HQ Ramstein und vermutlich auch an anderen Stellen im NS-System die kommerziellen (und nicht mehr ganz neuen) Serverbetriebssysteme Solaris 10 oder Windows 2003 sowie Software wie Oracle Java, Adobe Acrobat, Netscape 7, Exceed und OpenOffice nutzt. Diese Betriebssysteme und Software sind weit verbreitet und prinzipiell verwundbar in einem ausreichend hohen Maße[4], so dass davon auszugehen ist, dass professionelle Angreifer wie fremde Nachrichtendienste über mehrere vorgefertigte Angriffe auf diese Strukturen verfügen, die von normalen Sicherheitsmechanismen und Updates kaum betroffen sind. Sofern NATO also nicht systemweit alle nun bekannten Strukturen austauscht, sind Zugänge über diese Vektoren leicht möglich, auch bei erfolgten Änderungen der Passwörter und der Adresskonfigurationen.

Es ist hier anzumerken, dass es natürlich auch nicht so viele Alternativen für die Konstruktion von Servern und Netzwerken gibt, da der Markt stark von Marktführern dominiert wird, so dass also mit dieser Abbildung der Verwundbarkeiten prima facie nur eine Zeitersparnis für einen Angreifer geliefert zu sein scheint, der sonst auch auf solche Strukturen testen kann. Secunda facie ist aber anzumerken, dass solche Tests nicht einfach sind, dass Angreifer über diese Tests entdeckt werden können und dass solche Tests gute Rückkanäle erfordern. Eine genaue Kenntnis der Systemstrukturen ermöglicht also eine

---

[4] In offen dafür zugänglichen Datenbanken wie der Exploit Database (www.exploit-db.com) oder der National Vulnerability Database der NIST/DHS (web.nvd.nist.gov) finden sich bereits zahlreiche bekannte Schwachstellen zu den erwähnten Produkten, wobei davon auszugehen ist, dass mehrere hundert bis mehrere tausend weitere und noch unbekannte Verwundbarkeiten in den Produkten existieren.

wesentlich schnellere, risikoärmere Angriffspräparation und Angriffskonfiguration sowie ein sonst sehr aufwändiges Erstellen vollständig automatisierter Angriffe (dazu später mehr). Dies fällt besonders problematisch mit dem zuvor erwähnten Punkt der lateralen Bewegung zusammen, da ein Angreifer mit Kenntnis dieser Strukturen inzwischen bereits mehrere vorgefertigte tiefere Zugänge (sog. "Backdoors") oder fertige Angriffe weit im NS-System verteilt haben könnte.

Zusammenfassend lässt sich zur Basisoption des Zugangs sagen, dass dieser im Vergleich zur einfachen, äußeren Störung für professionelle Angreifer in der Regel um einiges interessanter ist, da ein Zugang einige interessante Folgeoptionen eröffnet, die taktisch besonders effektiv sind. Diese taktischen Folgeoptionen sollen im nächsten Abschnitt 1.2 gesondert als durch die betroffenen Informationen ermöglichte Operationstypen geschildert werden.

Zur Option des Zugangs sind abschließend noch Bemerkungen zu Zugangserweiterung und Zugangsverstetigung anzufügen. Ein Zugang wird in der Regel zunächst dazu genutzt werden, den Zugang zu vertiefen und zu verstetigen. Eine Vertiefung und Erweiterung findet statt, indem der Angreifer versucht, mit dem ihm gelungenen Zugang weitere Zugänge zu entdecken, indem er für andere, verbundene Ziele etwa weitere Passwörter oder verwundbare Systemstrukturen entdeckt, oder weitere Zugänge selbst anzulegen, indem er bei entsprechend hohen Privilegien selbst neue Nutzer und Administratoren anmeldet oder eigene Schadsoftware installiert. Im vorliegenden Fall ist beides leicht möglich, da die vorliegenden Strukturen sehr ähnlich sind, einen ähnlichen Aufbau, damit ähnliche Verwundbarkeiten, und vor allem eine sehr generische Passwortkultur offenbaren und da über die Root-, die Admin- und die EEPROM-Passwörter ein ausreichend tiefer Systemzugang ermöglicht wurde, um neue Zugänge anzulegen. Es ist also recht wahrscheinlich, dass Zugangsmöglichkeiten für andere NATO-Systeme erraten (oder wenig aufwändig ertestet) und angelegt werden können, so dass die erwähnte laterale Bewegung im gesamten NS-System möglich wird.

Hier ist bereits dringend anzumerken, dass die Passwortkultur der NATO herausragend schlecht ist. Die Passwörter verstoßen gegen jede mögliche Regel einer Passwortkultur, inklusive der eigenen Regeln der NATO zu Passwortkultur nach deren eigenen Information Security Vorschriften und sind tatsächlich ohne technische Hilfsmittel zu erraten. Dies ist eine extrem und vollkommen unverantwortlich grobe Sicherheitsverletzung von Seiten des IT-Personals der NATO, die erheblichen Anteil an dem möglichen Ausmaß der Folgeschäden des Vorfalls hat.

Eine Verstetigung wird in der Regel erreicht, indem ein Angreifer sich eigene Zugänge legt, die sich möglichst außerhalb des Erwartungs- oder des Einflussbereichs des Opfers befinden, um sie später und unabhängig vom bestehenden Zugang zu nutzen. Ein Angreifer, der über das Root-Passwort verfügt, kann aber auch andere Dinge tun, wie etwa schadhafte Software im Zielsystem zu installieren, die Systemänderungen zum Schutz des Systems vor Angreifern oder zur Detektion des Angreifers nur noch scheinbar oder gar nicht zulässt. Mit der lateralen Verbreitung und den Vorabinformationen über die technisch verwundbaren Strukturen könnten also bereits einige verstetigte Zugänge und Zusatzprogramme NS-systemweit installiert sein, wobei dies allerdings zum Teil den Informationen des KLAG geschuldet ist, zum Teil der extrem schlechten generischen Passwortkultur der NATO.

1.2 Varianten von Operationen durch Zugang

Die folgenden Ausführungen weisen Operationen aus, die mithilfe eines Zugangs in Zielsystemen durchführbar sind. Es sind erneut Basisoptionen, die in verschiedenen Systemen mit unterschiedlichen Inhalten und Systemfunktionen ganz unterschiedlich ausgeführt werden können und die taktisch kombiniert werden können.

1.2.1 Spionage

Hat man Zugang zu einem System mit bestimmten Rechten, so kann der Angreifer die unter diesen Rechten verfügbaren Informationen einsehen und kopieren, beziehungsweise versenden, und so Spionage betreiben. Cyberspionage kann sich auf verschiedene Informationstypen beziehen:

- explizite Informationen, die im System auch als solche explizit vorhanden sind, etwa Texte, Befehle, Kommunikationen oder in Command & Control Umgebungen die für die Command & Control Prozesse notwendigen Informationen über Bewegungen von fremden und eigenen Einheiten,

- implizite Informationen, die aus den im System explizit vorhandenen Informationen unter weiterem analystischem Aufwand gefolgert werden können,

- Metadaten, die über das System als Zusatzdaten etwa über Erstellungen oder Verwendungen der Dateien angelegt werden,

- Systeminformationen, die weitere Informationen über das angegriffene IT-System liefern und einen tieferen Zugang ermöglichen.

All diese Informationen sind verschiedentlich taktisch nutzbar. Sie geben einem Angreifer je nach Eindringtiefe ein genaues Bild von den Fähigkeiten und den Aktivitäten des Opfers, dessen organisatorischen und technischen Strukturen, von kritischen Verwundbarkeiten, von Prozeduren und Personen.

Bedingung für eine effektive Nutzung eines Zugangs zu Spionagezwecke ist allerdings ein Rückkanal. Hat ein Angreifer nur Zugang auf ein Netzwerk, so dass er dort hinein kann und dort Informationen oder Befehle platzieren kann, ohne dass es aber eine Möglichkeit gibt, aus dem System auch wieder Informationen zu extrahieren, so fällt Spionage als Option aus. Dies gilt etwa für physisch separierte Netzwerke, bei denen man über einen fingierten externen Datenträger zwar reinkommen kann, bei denen man aber über keinen festen Rückkanal verfügt, da eben keine Datenleitung nach Außen zurück zum Angreifer existiert.

Ein Angreifer kann allerdings verschiedene Taktiken anwenden, um dennoch an seine Informationen zu kommen. Er kann:

- einen Innentäter mit hohen Privilegien nutzen,

- vergessene oder nur scheinbar physisch separierte , in Wirklichkeit aber durchlässige Netzwerkstrukturen finden und nutzen,

- Extraktionspunkte an verwundbaren Punkten oder der Peripherie des Zielsystems festlegen, die es im vorliegenden Fall zahlreich zu geben scheint und die er über Innentäter erreichen kann, so dass an diesen Stellen die Informationen gesammelt werden,

- seine Angriffe automatisiert dazu anweisen, regelmäßig gestohlene Informationen auf Wechselmedien oder in Dokumente zu kopieren, um dann bei einem möglichen Anschluss dieser Wechselmedien oder Dokumente an ein offenes Netz die Informationen geschickt zu bekommen,

- versuchen, selbst einen externen Netzwerklink einzubauen.

Ein Rückkanal wird in jedem Fall interessant sein, vor allem, wenn es sich um einen möglichst direkten Rückkanal handelt, da in diesem Fall in Echtzeit auf Informationen zugegriffen werden kann, was im Falle eines Angriffs taktisch sehr gut genutzt werden kann.

1.2.2 Manipulation

Militärisch interessant ist an einem Zugang neben der Spionage vor allem die Manipulation der angegriffenen Systeme. Verschiedene Varianten der Manipulation sind möglich.

1.2.2.1 Ohne Rückkanal

Besteht kein direkter Rückkanal zum Angreifer, so können Manipulationen nur automatisiert ablaufen. Automatisierte Manipulationen werden im Offensivjargon auch als "Fire and Forget"-Angriffe bezeichnet. Ein Beispiel für einen automatisierten Angriff ist der bekannte Vorfall "Stuxnet", bei dem ein geschlossenes Netzwerk mit einem vollständig automatisierten Angriff erfolgreich angegriffen wurde. Für einen derartigen Angriff muss die Struktur des Ziels möglichst genau bekannt sein, damit die Angriffe auch ohne die Möglichkeit der nachträglichen Steuerung ohne Störungen oder Abstürze der Angriffssoftware ablaufen können. Dabei bestimmt die Art des Angriffs, welche Details über das System bekannt sein müssen, wobei Angriffe aber auch opportunistisch nach den vorhandenen Informationen gestaltet werden können.

Im vorliegenden Fall könnten aufgrund der betroffenen Informationen zu den technischen Systemen und möglichen Verwundbarkeiten dieser Systeme vollständig automatisierte Angriffe in das System eingebracht worden sein, die etwa weitere Zugänge legten oder aber automatisierte Manipulationen installiert haben.

Automatisierte Manipulationen können die folgenden Varianten annehmen:

- laufende Manipulationen können ab automatisierter Installation kleine Manipulationen am System vornnehmen, um Unschärfen oder Störungen einzubringen oder um kumulative Schäden zu verursachen, die zu einem späteren Zeitpunkt kritische Ausmaße annehmen können,

- logische Manipulationen können installiert werden, initiieren sich allerdings erst, wenn bestimmte logische Bedingungen eingetreten sind. Eine bekannte Variation wäre etwa eine "Time Bomb", die zu einem festen Zeitpunkt initiiert wird. Eine taktisch bessere Variation dagegen wäre eine "Logic Bomb", die unter anderen Bedingungen aktiviert wird und gut vom Angreifer genutzt werden kann. Denkbar ist etwa, dass eine Zivilmaschine mit einer bestimmten zivilen Kennung als logische Bedingung angegeben wird, wobei kurz vor einem Angriff diese Maschine das erste Mal losgeschickt wird, so dass sich daraufhin das C&C System der NATO Ramstein automatisch abschaltet oder - schlimmer - Signale verfälscht und einen friedlichen Zustand (oder einen anderen Angriff) vortäuscht, bis es für Reaktionen zu spät ist. Viele Manipulationen streben die Erreichung eines solchen "Point of No Return" an, da damit der Gegner nicht mehr handlungsfähig ist. Im vorliegenden Fall kann davon ausgegangen werden, dass

ein Angreifer zur Konstruktion eines solchen Angriffs befähigt gewesen wäre, sofern er sich über die angegriffenen Strukturen auch Zugang zu den konkreten Operationsweisen des ICC, des NIRIS, des JChat oder des FAST verschaffen konnte, was durch die offengelegten Informationen ebenfalls prinzipell möglich war, sofern Zugang zu den NS-Strukturen und ein Rückkanal vorhanden waren.

Die konkreten taktischen Optionen für logische Manipulationen sind je nach technischer und operativer Komplexität und Kritikalität des manipulierbaren Zielsystems äußerst zahlreich und kaum im Vorfeld vollständig abschätzbar.[5] Einige Varianten für C&C-Systeme werden weiter unten aufgeführt.

1.2.2.2 Mit Rückkanal

Sollte sich ein Rückkanal herstellen lassen, über die oben bereits erwähnten Mechanismen, wobei ein Innentäter bei der Größe des NS-Netzwerkes der wahrscheinlichste Rückkanal sein wird, so müssen Manipulationen nicht voll automatisiert sein. Sie können - je nach Qualität des Rückkanals - betreut, gewartet und ereignisspezifisch reaktiv betrieben werden. Auf diesem Wege sind dann wesentlich bessere und schwerer zu erkennende Angriffe möglich, da jedes Fehlverhalten der Angriffssoftware korrigiert werden kann und da deutlich spezifischer agiert werden kann. Auch ist so eine laterale Ausbreitung der Manipulationen und eine längere Lebensdauer der Möglichkeit der Manipulation von bis zu einigen Jahren möglich (selbst in Hochsicherheitssystemen und unter permanenten Sicherheitsprüfungen).

Des Weiteren gilt es, zwei inhaltliche Varianten von Manipulationen zu unterscheiden.

1.2.2.3 Manipulation von Informationen

Zuerst ist die Manipulation von Informationen in einem System zu beachten. Dies ist sowohl durch automatisierte wie durch über Rückkanal durch einen Operateur gesteuerte Angriffe möglich. Bei diesen Angriffen, die zum Teil auch als "Information Operations" oder "Electronic Warfare" oder "Signals Intelligence" bezeichnet werden (ebenso wie die folgende Kategorie), werden die durch das IT-System verarbeiteten und dargestellten Informationen verfälscht, um so falsche Einschätzungen und Lagebilder bei den bedienenden Operateuren zu generieren und diese zu zeitlich unpassenden oder falschen Entscheidungen zu verleiten. Dabei ist es wichtig anzumerken, dass die Abhängigkeit der Kommandeure

---

[5] Es wird spekuliert, ob die Ausschaltung der syrischen Luftabwehr im Rahmen der "Operation Orchard", einem israelischen Angriff auf ein syrisches Atomkraftwerk, durch eine logischen Manipulation des Systems erreicht wurde. Allerdings sind die Details dazu geheim.

von informationstechnisch aufgearbeiteten Lagebildern hoch kritisch ist und dass die Systeme unglücklicherweise häufig zentral oder hierarchisch anzugreifen sind, so dass also bei Fehldarstellungen, die an der richtigen Stelle platziert wurden, kein unabhängiger Kontrollkanal mehr besteht. Die Integrität dieser Systeme ist folglich unverzichtbar für die Funktion der NATO. Auch die Verfügbarkeit dieser Systeme ist kritisch. Für operative Belange kann es bereits zu einer kritischen Situation kommen, wenn Informationen verzögert dargestellt werden. Hierfür gibt es zahlreiche Optionen auf den C&C-Strukturen der NATO, durch die von KLAG bereitgestellten Informationen, sowohl als allgemeine Installationen für spätere Verwendungen wie auch bereits für damals laufende Operationen auf den damals aktiven Servern.

Folgende Operationen könnten durch die von KLAG offen gelegten Informationen an den NATO Informationen durchgeführt werden:

- FUD (Fear Uncertainty Doubt): ein Angreifer könnte durch gelegentliches Streuen von Fehlinformationen mit typischen Fehlermustern Zweifel an bestimmten Informationstypen produzieren, die folgend für verzögerte oder falsche Entscheidungen sorgen,

- Verzögerungen: ein Angreifer kann den Fluss kritischer Informationen kritisch verzögern. Ein solcher Angriff hätten den Vorteil, besonders unauffällig zu sein. Kritische Verzögerungen können leicht systembedingt sein,

- operativ kritische Fehlinformationen: ein Angreifer kann situationsspezifisch operativ kritische Fehlinformationen eingeben oder bestehende Informationen zu Fehlinformationen verfälschen. So ließen sich etwa Freund/Feind-Kennungen vertauschen, Orte und Zeiten, Angriffe könnten komplett ausgeblendet werden oder komplett vorgetäuscht werden, um Aktionen zu provozieren,

- taktisch geleitete Fehlinformationen: Fehlinformationen könnten außerdem auch weniger situations- und stärker taktisch gebunden eingesetzt werden, im Verbund mit weiteren Maßnahmen informativer oder sogar kinetischer Art.

Jede der zuvor genannten Manipulationen der Informationen hätte für die NATO leicht katastrophale Auswirkungen, aufgrund der bereits erwähnten hohen Abhängigkeit von diesen Informationen. Zudem hätten Fehlinformationen ein hohes Potential, systemweite kritische Fehlreaktionen und Verzögerungen zu bewirken, da das Funktionieren der NATO insgesamt durch das Paradigma der Network-Centric Operations stark miteinander vernetzt und voneinander abhängig ist. Es gibt hier zwar natürlich

entsprechende Pläne, um bei Fehlern und Ausfällen zu agieren, geschickte Manipulationen allerdings könnten eine sehr viel katastrophalere Wirkung haben.

1.2.2.4 Manipulation von Steuerungen

Neben Informationen können über Zugänge auf IT-Strukturen auch direkt Steuerungen von Maschinen angegriffen werden. Im vorliegenden Fall ist allerdings unbekannt, ob die durch die betroffenen Server verwendeten Daten auch direkt in Maschinen wie etwa in Fly By Wire -Systeme von Kampfflugzeugen eingespeist werden. Von daher sind einige der folgenden Bemerkungen unter diesem Vorbehalt zu bewerten. Die folgenden Manipulationen von Steuerungen sind denkbar:

- Steuerung der IT-Systeme (Datenmanipulation): in diesem Fall würde ein Angreifer die IT-Systeme selbst in ihren Funktionalitäten manipulieren, so dass bestimmte Funktionen entweder nicht mehr oder typisch und logisch prädisponiert fehlfunktionieren.

- Innere Störung: als Subtyp dieser Variante von Manipulation kann eine Störung der Systeme gesehen werden, die in diesem Fall nicht wie die oben erwähnte einfache Störung von außen kommt, sondern die von Innen ausgeführt wird und damit wesentlich feiner und präziser agieren und nur bestimmte Dienste unter bestimmten Bedingungen stören kann,

- Innere Zerstörung: gleicht der inneren Störung, löscht aber ohne Unterschied sämtliche Daten und Programme,

- Fehlsteuerung: sollten die betroffenen Systeme auch direkt Waffensysteme, Plattformen oder Flugsysteme mit direkt maschinell verarbeiteten Steuerungsdaten versorgen, ist auch eine direkte Manipulation dieser Steuerungsdaten denkbar. Ein Angreifer würden dann unabhängig von der Manipulation der Wahrnehmung und Entscheidung durch Informationsmanipulation noch eine Manipulation der von den C&C-Systemen ausgehenden Steuerungsdaten vornehmen, so dass also die Maschinen nicht nach dem Willen der NATO agieren, sondern nach dem Willen des Angreifers. Ein einfaches Beispiel wäre ein "-1"-Angriff, bei dem bestimmte Koordinaten mit Minus Eins multipliziert werden und damit in die exakt entgegengesetzte Richtung gesteuert werden. In einem Fall in Südafrika hat eine auf diese Weise fehlerhafte Software ein Geschütz bei einer Demonstration nicht auf ein Testziel, sondern auf das hinter dem Geschütz stehende Batallion feuern lassen.

- Taktisch geleitete Fehlsteuerung: auch in diesem Fall gilt, dass Manipulationen dieser Art im taktischen Verbund mit anderen Aktivitäten ausgeführt werden können.

Neben der Manipulation der C&C-Systeme für Raketenabwehr, für die NATO Luftwaffe und für die NATO Marine ist auch eine Manipulation der Applikationen JChat und FAST als kritisch zu bewerten, da auf diesen Wegen ebenfalls operativ kritische Funktionen für Einsätze realisierte werden. Dazu soll später noch mehr auf den technisch-spezifischen Punkten gesagt werden.

In jedem Fall gilt, dass eine Manipulation attraktiver ist als eine reine Störung und dass eine feingranularere Manipulation mit Rückkanal attraktiver ist als eine grobe und vollautomatisierte Manipulation. Alle Fälle werden durch die von KLAG verfügbar gemachten Informationen prinzipiell ermöglicht, wobei allerdings bei den besseren Varianten von Manipulationen zusätzliche Arbeitsschritte des Angreifers unternommen werden müssen.

1.3 Beschaffung und weiteres Targeting

Neben der Störung und dem Zugang und den damit verbundenen taktischen Aktivitäten nehmen Angreifer noch weitere Optionen typischerweise wahr, die im vorliegenden Fall ebenfalls ermöglicht wären.

Eine weitere wichtige Option bei einem einmal gelegten Zugriff ist die weitere Auskundschaftung des Zielsystems. Dies gelingt je nach Systemstruktur unterschiedlich gut. Beim betroffenen System ist davon auszugehen, dass eine weitere Auskundschaftung nicht zu schwer ist, sofern der Angreifer über einen Rückkanal verfügt, da die inneren Schutzmechanismen innerhalb des NS-Systems nicht sehr weitgreifend zu sein scheinen.

Noch wichtiger ist die Beschaffung dort befindlicher kritischer und nicht kommerziell am freien Markt erhältlicher Software, um in dieser Software einige der dort typischerweise häufig vorkommenden Schwachstellen zu identifizieren, die folgend für weitere Zugriffe und Angriffe auf diese Software im Kontext der Systeme genutzt werden können. Dieser letzte Punkt ist für den vorliegenden Fall besonders wichtig, da ein Angreifer über die durch KLAG zur Verfügung gestellten Informationen weiß, welche Software er an welchem Ort beschaffen kann. Eine erfolgreiche Exfiltration hängt dabei natürlich an dem Vorhandensein eines Rückkanals ab. Hat man allerdings Software oder genaue Kenntnisse über Verfahrensweisen wie zu JChat, FAST, NIRIS oder ICC erfolgreich beschafft, kann man folgend deutlich spezifischere Angriffe dafür schreiben und diese in das System an diesen Stellen einbringen.

In diesem Kontext ist es wichtig, auf den als weniger wichtig eingestuften Server OGAU hinzuweisen. Dieser Server enthält zum Testbetrieb und zu Schulungszwecken die operativ kritische Software JChat und FAST, die folglich auch von dort besorgt werden könnte, wobei davon auszugehen ist, dass die Sicherheitsvorkehrungen an dieser Stelle aufgrund der fehlerhaften Einschätzung, es hier nicht mit kritischen Systemen zu haben, niedriger sein könnten.

Folgende Software wäre taktisch wichtig zu beschaffen:

- JChat,

- FAST,

- NIRIS Software oder Verfahren,

- ICC Software oder Verfahren.

1.4 Weitere Bemerkungen zur Bewertung der Informationen durch Angreifer

Nach der allgemeinen Darstellung der Kernprobleme soll im Folgenden noch auf einige weitere Aspekte eingegangen werden, die für den vorliegenden Fall ebenfalls als relevant zu erachten sind.

1.4.1 Wichtige Merkmale hochwertiger nachrichtendienstlicher Angriffe auf Hochsicherheitssysteme

Folgend sollen einige typische Merkmale hochwertiger nachrichtendienstlicher Angriffe auf Hochsicherheitssysteme genannt werden, die möglicherweise auch auf dem durch die Informationen des KLAG möglicherweise kompromittierten NS-Netzwerk der NATO (gesamt, nicht nur HQ) zu erwarten sind.[6]

- Laterale Ausbreitung: Bereits mehrfach erwähnt wurde die Option der lateralen Ausbreitung. Ein professioneller Angreifer in einem hochwertigen Ziel würde mitunter zuerst eine maximale Ausbreitung anstreben, um an vielen verschiedenen Punkten des Systems zu sitzen und damit schwerer zu beseitigen zu sein. Sollte ein Angreifer für einige Zeit (etwa zwischen einem Monat und drei Monaten) Zugang auf

---

[6] Diese Merkmale können in der Literatur unter dem Stichwort "APT" (Advanced Persistent Threat) recherchiert werden. Mit APTs werden gemeinhin militärische oder ähnlich hochwertige Angriffe bezeichnet.

die NATO NS-Systeme gehabt haben, wäre davon auszugehen, dass er sich lateral in diesem System bewegt hat und inzwischen an vielen Stellen des Systems sitzen kann. Die laterale Bewegung wurde im vorliegenden Fall durch die schlechte Passwortkultur und durch die Kenntnis der Infrastrukturen und die damit naheliegenden Rückschlüsse auf weitere Struktruen des NS-Netzes zusätzlich begünstigt.

- Multiple, heterogene Angriffe und schlafende Backdoors: Ein professioneller Angreifer würde in einem hochwertigen Ziel zudem verschiedenartige Angriffsvorbereitungen oder automatisierte Angriffe sowie heterogene Typen weiterer Zugänge (Hintertüren) legen, im Kontext einer lateralen Bewegung.

- Tarnung: Ein professioneller Angreifer würde zudem ein maximales Gewicht auf eine gute Tarnung legen. Eine frühzeitige Entdeckung eines Angriffs oder einer Hintertür ist für einen Angreifer immer mit Kosten und Risiken verbunden. Daher wird in der Regel viel Entwicklungsaufwand auf die Tarnung und die Störungsfreiheit der Angriffe gelegt. Angriffe professioneller Angreifer in Hochsicherheitsstrukturen sind teilweise trotz ausgereifter Sicherheitstechnologien über Jahre nicht zu entdecken.[7]

- Darknets: Ein gut getarnter, lateral verbreiteter Angriff kann zudem wie ein eigenes Netzwerk mit verteilten Funktionen betrieben werden, wobei (1) überall im System Informationen gesammelt oder manipuliert werden können, (2) einige Teile des versteckten Angreifernetzwerkes ("Darknet") mit besonderen Funktionen wie Tarnung oder Exfiltration beauftrag werden können, was diese Prozesse effizienter macht, (3) Schwachstellen im System effizienter ausgenutzt werden können und (4) Angriffe sogar reinstalliert werden können, wenn sie vom Opfer entdeckt und deinstalliert werden. Ein professionelles Team mit gutem Zugang zu einer Zielstruktur kann innerhalb kurzer Zeit Grundzüge eines solchen Darknets anlegen, so dass auch diese Option in Betracht gezogen werden kann.

- Anzunehmende Vorbereitung professioneller Cyberangreifer: Professionelle Cyberangreifer produzieren zudem viel Cyberangriffe auf Vorrat, besonders für gängige Typen kommerzieller Ziele. Da die betroffenen Systeme stark durch kommerzielle, gängige Systeme konstituiert werden (Sun Solaris, Java, Acrobat, OpenOffice, Windows), ist davon auszugehen, dass professionelle Angreifer bereits über eine Reihe vorbereiteter Angriffe auf diese Strukturen verfügen. Dies ist im vorliegenden Fall relevant, da die Angreifer so nur ein kleines Zeitfenster benötigen, um ihre Angriffe ins Ziel einzubringen und anzupassen.

1.4.2 Mögliche Angreifer

[7] Die Vorfälle Flame, Duqu und Red October sind hier gute Beispiele.

Bei den offen gelegten Informationen muss beachtet werden, dass sie von Akteuren unterschiedlicher Qualität genutzt werden könnten. Auf dem oberen Ende dieses Akteursspektrums stehen hochprofessionelle Angreifer wie russische oder chinesische Nachrichtendienste, die sämtliche der erwähnten Optionen wahnehmen können. Hier ist von einem hohen Schaden auszugehen, sollte einer der erwähnten Akteure tatsächlich oder auch nur möglicherweise Zugriff auf einige dieser Daten gehabt haben. Diese Akteure wären vorbereitet gewesen und hätten nur wenig Zeit benötigt, um die Systeme der NATO dauerhaft, lateral weit ausgebreitet und kaum sichtbar zu infiltrieren und damit gegen diese Gegner unbrauchbar zu machen. Aber auch andere Akteure hätten mit den Daten viel anfangen können. Als weniger qualifizierte Akteure wären die Taliban oder Terroristen zu nennen, die mit den Informationen immerhin noch Zugriff hätten erlangen können und die einige vollautomatisierte Angriffe zu kritischen Zeitpunkten hätten absetzen können. Es bestehen berechtigte Zweifel, ob die NATO gegen eine innere Störung durch einen automatisierten Angriff von Außen gewappnet wäre.

1.4.3 Aktualität von Informationen, Backups und Testumgebungen

Aktuelle Informationen sind allgemein wertvoller als Informationen über inaktive Server oder veraltete Informationen. Veraltete Informationen können Angreifer sogar zu falschen Schlüssen führen und zu einer Entdeckung möglicher Angriffe führen, was ein Vorteil für die Verteidigung wäre. Aus dieser Perspektive sind die zu Project 36 verfügbar gemachten Informationen für Angreifer besonders wertvoll, sofern der Angreifer diese Informationen richtig bewertet. Es können allerdings auch veraltete Informationen noch wichtige Hinweise zur Struktur des Zieles geben, indem dort etwa Hardware und Software genannt werden, die vermutlich in ähnlichen Formen auch in neuen Konfigurationen weiter verwendet werden.

Backups sind in diesem Kontext anders zu bewerten. Backups ebenso wie Testumgebungen (wie OGAU) stellen reale Systemkonfigurationen dar, auch wenn die konkreten Daten nicht "echt" sind. Damit werden also trotzdem angriffsrelevante Informationen preisgegeben, wie Hardware und Software. Software kann teilweise auf diesem Weg auch entwendet und auf Schwachstellen getestet werden. Zudem sind Backups teilweise schlechter gesichert, was für Angreifer die Option eröffnen kann, die Backups zu infizieren und dann durch Störangriffe auf die Originalsysteme einen Wechsel der Operationen auf die infizierten Backups zu erzwingen. Dies wurde in der Praxis bereits beobachtet.

1.4.4 Budgetinformationen

Die offen gelegten, allerdings ohnehin nicht klassifizierten Budgetinformationen sind nicht feingranular genug, um besonders wertvolle Hinweise für Angreifer zu entbergen. Sie legen allerdings offen, dass allgemein nicht viel Geld für die IT-Sicherheit der NATO ausgegeben wird. Bestimmte teure Sicherheitsmechanismen können auf diesem Weg ebenso ausgeschlossen werden wie zahlreiches hochqualifiziertes Personal. Dies sind allerdings Standardbedingungen, von denen Angreifer gegenwärtig ohnehin ausgehen. Daneben wären Budgetinformationen interessant, um Subunternehmer und Supplier der NATO-IT sowie outgesourcte Dienste zu erkennen. Bei solchen externen Akteuren ist es in der Regel leichter einzudringen und Angriffe zu platzieren, die dann über diese Akteure in das gesicherte System eingetragen werden. Solche Angriffsvektoren werden auch als Supply Chain-Vektoren bezeichnet.

1.4.5 Kombination mit offenen Informationen

Im Kontext des Ermessens eines möglichen Schadens der NATO ist zudem noch einzubeziehen, dass die entwendeten als GEHEIM zu klassifizierenden Informationen durch die entwendeten offenen Informationen über Emails und das PAN-System für einen Angrifer hilfreich ergänzt werden. So ergibt insbesondere die Verbindung offener und geschlossener Informationen ein recht umfangreiches Bild von der NATO, mit vielen Angriffsvektoren. Dazu sollen noch die folgenden Bemerkungen gemacht werden:

1.4.5.1 Email-Adressen

Eine Liste von Email-Adressen ist für einen Angreifer nützlich und wichtig, da (1) damit eine Abbildung von Zielpersonen angelegt werden und da (2) nach dieser Abbildung von Zielpersonen eine Manipulation der Zielperson erfolgen kann, wobei hier insbesondere (3) das Versenden einer infizierten Email über sogenanntes "Spearphishing" oder über einen Phishingangriff erfolgen kann. Die Liste der Adressen ist nicht eingestuft und kann unter Umständen auch einfach über das Internet abgefragt werden wie etwa durch Google-Suchen oder über spezifische Programme wie "The Harvester". Dies kann allerdings auch schwierig sein, wenn Schutzmaßnahmen ergriffen wurden oder wenn - wie in diesem Falle anzunehmen ist - viele veraltete Informationen mit unklarer Zugehörigkeit im offenen Internet vorhanden sein werden. Ein Test dahingehend wurde nicht unternommen. Die Liste stellt allerdings bei Aktualität in jedem Fall eine Erleichterung der Angriffsvorbereitung dar.

1.4.5.2 Abbildung von Zielpersonen

Da die Email-Adressen der NATO die Klarnamen der Empfänger beinhalten, ist es über die Liste möglich, die realen Personen zu identifizieren und sie im Internet oder über konventionelle Spionage ausfindig zu machen und in einem Profil abzubilden. Diese Profile enthalten mitunter viele hundert Informationen

und geben ein genaues Bild von den beruflichen und privaten Ausdehnungen einer Person. Insbesondere dann, wenn die Person noch häufig digitale Medien des Web 2.0 nutzt und sich intensiv über Facebook und ähnliche Webdienste mitteilt, können viele Informationen gewonnen werden.

Für Cyberangriffe sind solche Informationen wichtig, um Zugangsvektoren zum Ziel zu schaffen. Einmal können so Innentäter identifiziert werden, die später Angriffe in das geschlossene System bringen können. Dann können aber auch Spearphishing- und ähnliche Angriffe auf diese Weise vorbereitet werden. Dieser Punkt wird weiter unten noch ausgeführt.

1.4.5.3 Manipulation von Zielpersonen

Diese Informationen können folgend genutzt werden, um die Person zu manipulieren. Kompromittierende Informationen etwa können direkt zur Erpressung genutzt werden, während andere Informationen genutzt werden können, um Vertrauensverhältnisse zum Opfer aufzubauen, über das Vortäuschen falscher Interessen oder "Gemeinsamkeiten" durch einen digitalen oder realen Angreifer. Oft lassen sich über diesen Vektor auch nachrichtendienstlich besonders geeignete Opfer identifizieren, die möglicherweise einsam sind und einen Partner suchen, oder die mit ihrem Arbeitgeber oder ihrer finanziellen Situation unzufrieden sind. Entsprechende Personen sind leichter zu manipulieren.

1.4.5.4 Versenden infizierter Emails

Das Vorhandensein von Email-Adressen verleitet auch häufig zur Versendung von infizierten Emails. Solche Emails können leicht in geschlossene Systeme weitergeleitete werden, ohne dass die infizierten Anhänge von Virenscanner bemerkt werden müssen. Im vorliegenden Fall etwa wäre dies durch infizierte PDF-Dokumente oder OpenOffice-Dokumente möglich, da der Angreifer durch die Anweisungen zum Aufbau der Server genau weiß, dass diese für professionelle Angreifer als verwundbar geltenden Dateiformate verwendet werden.

Bedingung für das Durchkommen einer derart infizierten Email ist, dass sie für legitim gehalten wird. Dazu eigenen sich sogenannte "Spearphishing"-Angriffe. Bei diesen Angriffen bildet man vor dem Versenden einer infizierten Email das Opfer genau ab, um dann eine personalisierte Email mit höherer Glaubwürdigkeit abzusenden. Man spricht Interessen oder laufende Geschäftsprozesse an, verwendet mitunter einen zuvor gehackten Account eines Bekannten dafür und schickt so eine gefälschte Nachricht ab, deren Anhang dann im NS-System geöffnet wird.

Spearphishing-Angriffe sind im Hochsicherheitsbereich durchaus anzutreffen. Chinesische Rüstungsspionage etwa wurde bereits über Spearphishing-Angriffe mit vorbereitet. Sie werden allerdings nur selten eingesetzt, wenn von Nachrichtendiensten wirklich hochwertige Angriffe, basierend auf entsprechend hochwertigen Informationen, durchgeführt werden, da bei Spearphishing-Angriffen immer ein gewisses Risiko der Entdeckung besteht. Der Rezipient der Email könnte sich aufgrund einiger dem Angreifer unbekannter Informationen über den Inhalt wundern, beim Absender oder bei Kollegen nachfragen oder Folgehandlungen als Antwort einleiten. Gerade bei Emails, die persönlich betreffen sollen, kann das passieren. In diesem Fall würde der Angriff also solcher entdeckt werden. Wird ein Angriff entdeckt, sind einige Vorteile wie angeschaffte Informationen und einige Mittel wie teure Entwicklungsarbeiten der Angriffe, sowie Informationen über deren Methodik und ähnliches, dem Opfer bekannt und damit für den Angreifer wertlos. Zudem wird das Opfer von da an vorsichtiger sein.

Wahrscheinlicher sind daher andere Vektoren. Einer dieser Vektoren könnte allerdings auch über Email-Listen gehen. In diesem Fall würde man sich als Angreifer bemühen, das Netz möglicher Kontaktpersonen der NATO-Zielpersonen zu identifizieren, in deren in der Regel schlechter geschütztes Mailkonto einbrechen und dann eine echte Email von dort als "Man In The Middle" abfangen oder doppelt senden und anstelle eines echten Anhangs einen infizierten Anhang anfügen.

Ansonsten sind aber Innentäter oder Supply Chain Angriffe deutlich beliebtere Zugangsvektoren bei hochwertigen Angriffen auf hochwertige Ziele, da diese Angriffe zwar für die ausführenden Personen riskanter, sonst aber bei guter Vorbereitung wesentlich schwerer zu entdecken sind.

1.4.5.5 Strukturen des offenen Netzwerks

Die offengelegten Informationen zeigen auch verschiedene Informationen zum offenen PAN-Netzwerk. Diese Informationen sind nicht eingestuft und mit etwas Aufwand auch ohne eine besondere nachrichtendienstliche Beschaffung zu erhalten. Sie erleichtern allerdings einem Angreifer erste Arbeitsschritte. Ein Angreifer könnte drei Handlungen auf diese Weise erleichtert ausführen: Er kann (1) die offenen Systeme stören oder sich Zugang verschaffen und (2) die offenen Systeme beobachten und (3) Teile der offenen Systeme infiltrieren.

1.4.5.6 Störung der offenen Systeme

Sind die Adressen, die Zusammenhänge und einige der Konfigurationen des offenen Netzwerkes bekannt, kann dieses Netzwerk von Außen gestört werden. Beliebt sind hier insbesondere Ressourcenangriffe wie die bekannten "Denial of Service"-Angriffe, bei denen versucht wird, die

Kapazitäten des Systems durch massenhafte Anfragen oder rapide wiederholte Arbeitsprozesse so zu überlasten, dass das System für normale Betriebsanfragen nicht mehr ansprechbar ist.In der Struktur der NATO ist davon auszugehen, dass die Störungen keine missionskritischen Auswirkungen haben sollten. Allerdings werden im Hochsicherheitsbereich solche Störungen oft eingesetzt, um Ablenkungen zu generieren für andere Angriffe, die unter oder neben der Störung abgesetzt werden. Die gute Nutzbarkeit in diesem Kontext hängt damit zusammen, dass es in der Regel nur kleine Personalkontingente gibt, die sich überhaupt mit IT-Sicherheit beschäftigen, und dass diese Kontingente daher nicht nach geschlossen und offen getrennt sind. Das Team, das für den Schutz des geschlossenen Systems zuständig wäre, müsste also aller Voraussicht nach auch den offenen Angriff behandeln, wodurch sich andere Aktivitäten am geschlossenen System besser ausführen lassen.

Raffiniertere Störungen verzögern oder behindern den Betriebsablauf auf feingranularere Weise, umso länger personelle Ressourcen zu binden.

1.4.5.7 Zugang und Beobachtung oder Manipulation

Bei einem offenen System ist davon auszugehen, dass Angreifer über infizierte Emails und getarnt als normale kriminelle Cyberangreifer bei kommerzieller verwandter Software recht einfach Zugang erhalten können. Ist so ein Zugang erst einmal dauerhaft gelegt, kann er für verschiedene Zwecke genutzt werden. So kann etwa der Datenverkehr genau beobachtet und ausgewertet werden, was wieder Hinweise auf interessante Zwischenziele gibt oder als "Open Source" Intelligence weitere Hinweise auf geheimes oder fast geheimes Wissen geben kann. Dabei ist zu beachten, dass die Sicherheitskulturen oft nicht ausreichend hart sind, um wirklich vollständige Isolierungen von Geheimnissen zu erlauben. Insbesondere Geheimnisse auf der Stufe "Vertraulich" werden erfahrungsgemäß gelegentlich doch zur Arbeitsersparnis über offene Netzwerke versandt. Die Stufe "Vertraulich" ist für fremde Nachrichtendienste in der Regel wenig interessant, kann aber dennoch wichtige Indikatoren enthalten. Außerdem lässt sich so ein Profil der Zielorganisation und ihrer Kommunikation nach außen anlegen.

Neben der Beobachtung ist außerdem eine Manipulation der offenen Systeme möglich, derart, dass der Betriebsablauf nach Belieben des Angreifers gestört werden kann. Inwiefern eine Störung des offenen Systems den Betrieb des NS-Systems und die Operativität der NATO insgesamt stören kann, ist ohne eine operative Analyse nicht eindeutig zu sagen.

2. Konkrete Anmerkungen zu einzelnen Punkten der betroffenen Informationen

Im Folgenden sollen einige der konkreten Informationen in Bezug zum Vorangegangenen gestellt werden.

2.1 Nutzbarkeit einiger offengelegter technischer Informationen im Einzelnen

Racks: Hierdurch kennt ein Angreifer die physischen Orte der Server und kann etwa über Innentäter direkt an diesen Servern agieren, sofern er sich physischen Zugriff verschaffen kann.

Roles: Hierdurch wird dem Angreifer mitgeteilt, welche Server in welchen technisch-funktionalen Rollen arbeiten und damit auch, welche Abhängigkeiten in welchen Verhältnissen existieren und welche Funktionen überhaupt genutzt werden.

IP-Adressen, Gateways, DN-Informationen, Mask, Router IP, Host ID, Ethernet Address: Diese Informationen sind Informationen über den Aufbau der Netzwerke, die genaue Adressen, die Strukturen und die Beziehungen der Netzwerke wiedergeben.

Loopbacks: Loopback Adressen sind immer erreichbar und werden daher für die Konfiguration der Netzwerklogik verwendet. Sie sind für die Analyse der logischen Netzwerkorganisation sowie für Angriffe auf diese entscheidend.

Host Name: Diese Information gibt an, welchen Namen der Server hat, ist aber generisch gewählt, so dass gleichzeitig die Funktion damit preisgegeben wird.

VLANs, Virtual ESXI Servers: VLANs sind virtuelle Netzwerke, die auf physischen Netzwerken aufsetzen. Hat ein Angreifer Zugang zu einem physischen Netzwerke auf tiefer Systemschicht, kann er darüber alle virtuellen Netzwerke ansteuern und rein virtuelle Trennungen umgehen. Außerdem werden hier weitere Informationen über Netzwerkstrukturen und Abhängigkeiten weitergegeben.

Serverinfo Operating System: Hier werden die Betriebssysteme angegeben, auf denen die Server laufen. Alle der angegebenen Betriebssysteme sind kommerzielle Off The Shelf Produkte und gelten als gemeinhin verwundbar. Solaris 10 etwa ist ein nicht mehr ganz neues, aber weit verbreitetes Betriebssystem für Serverstrukturen. Es gilt als gut geeignet für einen sicheren Betrieb, trotzdem aber auch als verwundbar.

Server Model: Hier wird die Server Hardware beschrieben. Auch damit können taktische relevant Rückschlüsse gefolgert werden, indem etwa auch Hardware verwundbar sein kann (Firmware) oder indem bestimmte Betriebssysteme und Konfigurationen erforderlich sind.

Passwort Root, EEPROM, LDAP, ICC, Admin: Diese Passwörter erlauben den Zugang auf sehr frühen und sehr kritischen Prozessen, so dass hier besonders weitreichende, besonders schwer zu detektierende und besonders kritische Zugänge gelegt werden können.

Andere Passwörter: Die andere Passwörter sind rollen- der softwarespezifisch und weniger schädlich, erlauben aber trotzdem den je spezifischen Zugang.

Encrypted pw: Diese Passwort scheint zur Entschlüsselung von verschlüsselten Inhalten oder Diensten da zu sein. Je nach nachgelagertem Dienst kann die Kenntnis dieses Passwortes die Sicherheit kritisch beeinträchtigen.

Software: In den Build Anleitungen sowie in den Serverinformationen wird mehrfach die verwendete Software angegeben, was so dort vorhandene Verwundbarkeiten offenbart.

2.2 Spezifische Verwundbarkeiten der Systeme und Funktionen

JChat, FAST: Bei JChat und FAST wäre es für einen Angreifer interessant, spionieren und manipulieren oder stören zu können. Diese Dienste sind missionskritisch, offenbaren entscheidende taktische Momente und Lagebilder und können schon bei kleinen Störungen kritische Fehler in den Entscheidungsprozessen nach sich ziehen.

NIRIS: Das NIRIS System enthält nach Angaben der NATO operativ relevante und im Missionsfall kritische Informationen zu Luftlagebildern. Das System empfängt und sendet diese Lagebilder. Damit ist dieses System ein für potentielle Gegner kritisch relevantes System. Es ist überaus relevant für Spionage, um Stärken, Fähigkeiten, Manöver, Taktiken, Interessen und konkrete Aktivitäten eines Gegners zu beobachten und um mögliche Tarnungen nichtig zu machen. Und es ist überaus interessant für Manipulationen, da mit Manipulationen auf Lagebildern zahlreiche fehlerhafte Szenarien in die Command & Control Prozesse eingebracht werden können, die zu falschen Entscheidungen und zu kritischen taktischen Nachteilen führen. Indem das System Informationen nicht nur selbst verarbeitet, sondern auch versendet, können auch andere Teile der NATO auf diesem Wege ausspioniert und manipuliert werden.

MCCIS: Siehe NIRIS, wobei dieses System zusätzlich über Land- und Seelagebilder verfügt.

ICC: Das ICC ist dafür zuständig, militärische Kommunikations- und Entscheidungsprozesse zu organisieren und zu ermöglichen. Hier sind alle erwähnten Optionen für Spionage, Manipulation und Störung an Command & Control Funktionen für jeden Angreifer hochinteressant, da hier kritisch eingewirkt werden kann. Je nach Menge und Qualität der Informationen, die im ICC vorgehalten werden, können viele konkrete Planungen und Schemata von der möglichen Offenlegung betroffen sein, so dass diese Planungen und Schemata neu entworfen werden müssen.

ICCOPENVIEW: Die hier entborgenen Manöverinformationen können selbst bei veralteten Daten taktisch ausgewertet werden und damit taktisch relevante Informationen beinhalten, sofern der Server bei Inaktivität angesprochen werden konnte.

IS NS NIRIS: Hier sind konkrete Daten zu Luftbildern der ISAF-Mission in Afghanistan vorhanden gewesen. Der Server ist mit NATO Security Script gesichert gewesen. Da Zweifel an der Funktionalität des Security Script bestehen, kann nicht mit Sicherheit ausgeschlossen werden, dass die darauf befindlichen Daten nicht offenbart wurden. Waren die Daten noch gültig während der Tatzeit, so hätten sich damit die ISAF Missionen kritisch beeinflussen lassen. Taktisch kritische Informationen hätten an potentielle Gegner übermittelt werden können, der folgend taktisch besser hätte agieren können. Außerdem könnten im Weiteren strategische Informationen zu typischen Stärken, Schwächen und Vorgehensweisen verlorgen gegangen sein. Diese letzteren Informationen wären auch noch wertvoll, wenn der Server zur Tatzeit nicht mehr aktiv, aber ansprechbar gewesen ist.

OGAU: Wie bereits erwähnt könnte auf dem System OGAU aufgrund dort möglicherweise niedrigerer Sicherheitsmaßnahmen kritische Software abgezogen worden sein, und es könnten typische Vorgehensweisen der NATO beobachtet und abgezogen worden sein.

3. Schäden für die NATO

Im Folgenden sollen einige Bemerkungen zu möglichen Schäden für die NATO gemacht werden.

3.1 Strategische Schäden

Strategische Schäden entstehen der NATO in der Folge des Vorfalls, da potentielle Angreifer die ermöglichten Zugänge für die oben erwähnten operativen Zwecke nutzen könnten und zeitlich und in

ihrer Ausdehnung unbekannt weitgreifende Spionage, Störaktionen oder Manipulationen an unterschiedlichen taktischen Punkten unternehmen oder vorbereitet haben könnten. Besonders problematisch ist außerdem, dass in den Systemen nicht mehr festzustellen ist, ob sich dort in Folge des Vorfalls ein Angreifer eingenistet hat oder nicht. Insbesondere gegen hochwertige Angreifer gibt es keine auch nur ansatzweise zuverlässigen Testverfahren. Die Komplexität der in diesem Fall verwendeten kommerziellen Systeme verhindert dies. Es muss also von einer dauerhaften Unsicherheit ausgegangen werden.

Spezifisch aus Perspektive der Zugangsmöglichkeiten entstehen strategische Schäden, indem (1) ein Angreifer Informationen über das NATO-System konkret hätte nutzen können, um laufende Operationen zu beeinflussen, indem (2) ein Angreifer viele der Information voraussichtlich auch nach einer Reform der Sicherheitsstrukturen in Folge des Vorfalls nutzen kann, wie Informationen über Verwundbarkeiten in der verwendeten kommerziellen Hard- und Software, (3) indem ein Angreifer aus den Informationen gute Rückschlüsse über allgemeine technische Strukturen und Schwächen der IT der NATO ziehen kann, die noch für lange Zeit nutzbar sein könnten, (4) indem ein potentieller Angreifer durch laterale Bewegung und Tarnung aktuell bereits weit in dem NS-System verbreitet und kaum mehr zu entfernen sein könnte, so dass eine Unsicherheit über die Integrität der Systeme im Krisenfall verbleiben muss, bis die Systeme vollständig und möglichst zeitgleich ausgetauscht oder neu aufgesetzt werden, was mit erheblichen und mitunter nicht hinnehmbaren operativen Einschränkungen verbunden wäre.

In dieser Bewertung hängt viel daran, ob ein potentieller professioneller Gegner Zugang zu den Informationen erhalten haben könnte, ob er über weitere Innentäter oder andere Vektoren Zugriff auf das NS-System hatte oder ob er komplett von Außen hätte agieren müssen und wie groß das Zeitfenster gewesen sein könnte, um in den NS-Systemen zu arbeiten. Zum ersten Punkt des Zugangs ist festzuhalten, dass allein das Versenden über den ungeschützten, für professionelle Angreifer leicht offenen kommerziellen Mailanbieter GMX im offenen Internet die prinzipielle Gewährleistung eines solchen Zugangs bedeutet. Der GMX-Zugang könnte absichtlich oder versehentlich für mögliche Gegner zugänglich gewesen sein. Diese Bedingung ist also aus einer Perspektive der Defensive prinzipiell erfüllt. Zu der zweiten Frage eines potentiellen weiteren Innentäters oder Innenvektors lässt sich nicht viel sagen ohne weitere Erkenntnisse der Spionageabwehr, wobei allerdings aus einer reinen Cyberdefense-Perspektive wie bereits erwähnt davon auszugehen ist, dass bei einem entsprechend weit ausgedehnten System wie dem NATO NS-System direkte oder indirekte Innentäter mit gewissen Rückkanälen von unklarer Qualität anzunehmen sind. Dieser Punkt ist also zumindest nicht auszuschließen. Ein genaues Risiko lässt sich allerdings nicht angeben.

Zum letzten Punkt ist zu sagen, dass zwei Zeitfenster zu beachten sind: (1) zwischen der ersten falschen Ablage der sensiblen Daten im DHS und der Gegenreaktion im Juli 2012 und (2) zwischen den erfolgreichen Transfers der elf Dateien und dem Ausdruck der P36-Datei im März 2012 und der Gegenreaktion im Juli 2012.

Zeitraum (1) ist der sicherlich längste Zeitraum. Ohne genauere Kenntnis über weitere mögliche Übermittlungswege durch Datenübertragungen über Datenleitungen oder Wechselmedien könnte angenommen werden, dass KLAG oder eine andere Person die Daten bereits direkt nach dieser fehlerhaften Einstellung an einen potentiellen Gegner übermittelt hat, was ein großes Zeitfenster für potentielle Operationen erlaubt. Derartige alternative Übermittlungen könnten in anderen Ausdrucken, Transporten über Wechselmedien durch ungeschützte Anschlussstellen oder Datenübermittlungen in fingierten Dokumenten über das PAN-Netzwerk geschehen sein.

Aber auch der klar feststehende Zeitraum (2) muss als vollkommen ausreichend erachtet werden, sofern vorbereitete und professionelle Akteure als Gegner anzunehmen sind. Wie erwähnt haben solche Akteure in der Regel bereits weitere Innentäter, andere Rückkanäle und vor allem vorbereitete Angriffe auf die im NS-System vorhandenen Standardtechnologien. Für solche Akteure wäre es also ab Erhalt der Informationen nur eine Sache von einigen Tagen bis Wochen, einige effektive Zugänge oder Angriffe zu legen und erste laterale Bewegungen zu unternehmen, wobei nach einigen Wochen bis drei Monaten bereits ein effektives Darknet im NS-System betrieben werden könnte, das nicht mehr zu entdecken wäre. Von daher ist auch der Wert der Gegenreaktion zur Abwehr der durch den Vorfall entstandenen Schäden nicht als Abschluss des Vorfalls anzusehen.

In dieser Hinsicht ist außerdem noch anzumerken, dass einige Angriffe auch unabhängig von den Gegenreaktionen der NATO noch möglich sind. Hierzu zählen insbesondere Angriffe, die nicht über den offensichtlichen Weg der Passwörter gehen - diese sind eher eine Zeitersparnis - sondern über Verwundbarkeiten in der nun bekannten Soft- und Hardware. Sofern die NATO also diese Strukturen nicht austauscht, ist hier von einem noch offenen Fenster auszugehen.

Zusammenfassend lässt sich also sagen, dass die NATO sowohl konkrete operative Schäden an Leib und Leben in den damals auf den betroffenen Strukturen aktiven Missionen hätte davontragen können, dass aber auch in Zukunft durch den Vorfall nicht mehr sicher ausgeschlossen werden kann, dass konkrete operative Schäden in zukünftigen Missionen entstehen, die von den betroffenen oder analogen Strukturen aus betrieben werden. So ist der NATO mit dieser Unsicherheit auch ein großer strategischer Schaden zugefügt worden.

3.2 Monetäre Schäden

Monetäre Schäden entstehen auf mehreren Ebenen und je nachdem, als wie kritisch die NATO eine mögliche persistente und nicht zu entdeckende Kompromittierung einstuft. Als unmittelbarer monetärer Schaden ist der Aufwand des Setzens neuer Passwörter zu bewerten. Davon ausgehend können verschiedene weitere Sicherheitsmaßnahmen ergriffen werden wie eine Änderung der Netzwerkstrukturen und -adressen, der Abhängigkeiten und Kritikalitäten auf einem mittleren Level oder auf hohem Level der komplette Austausch der nun bekannten Soft- und Hardware, wobei dieser entweder nur auf dem HQ Ramstein stattfinden könnte oder systemweit im NATO NS-System. Zum Verfahren muss hier gesagt werden, dass es bei Militärs oft eher üblich ist, nach Systeminfektionen eher minimal zu reagieren (aus Kosten- und Personalgründen), während allerdings bei möglicher Kompromittierung durch einen gegnerischen Nachrichtendienst eigentlich die extrem erscheinende Variante eines vollständigen Wechsels aller potentiell verwundbarer Strukturen im gesamten NS-System stattfinden müsste. Es kann andernfalls nicht mehr sicher davon ausgegangen werden, dass diese Systeme nicht doch kompromittiert sind und im entscheidenden Moment versagen.

Zusammenfassend lässt sich hier also sagen, dass erhebliche monetäre Schäden an der NATO entstehen, sofern ein vollständiger Systemwechsel beschlossen werden sollte. In diesem Fall müssten alle betroffenen und analogen Strukturen der NATO ersetzt werden. In der Praxis ist allerdings oft ein nachlässiger Umgang mit diesen Recovery-Maßnahmen zu beobachten, so dass der reale Schaden weit unterhalb der Summen eines Austauschs liegen könnte.

4. Antworten auf die gestellten Fragen

4.1. Wäre eine unbefugte Person in der Lage, mittels der in den Dateien enthaltenen Informationen - insbesondere Passwörter und IP-Adressen - einen vollständigen Überblick über die Funktionsweise der betroffenen Computersysteme (Server) der NATO zu gewinnen und diese zu manipulieren?

Ja. Die Informationen sind ausreichend, um ein genaues Bild der Serverstrukturen des NATO HQ Ramstein und des NS-Netzwerkes allgemein zu erhalten. Ein potentieller Angreifer erfährt über diese Daten unmittelbar:

(1.1) wie die Server miteinander verbunden sind, was für ein Netzwerk unterhalten wird,

(1.2) zum Teil, welche Betriebssysteme, Software und Hardware eingesetzt werden,

(1.3) Passwörter und technische Adressen im NS-Netzwerk,

(1.4) Zuständigkeiten für Server,

(1.5) technische und operative Details zum Aufbau der Server.

Zudem kann ein potentieller Angreifer mit diesen Informationen in die Systeme eindringen und dort weitere Informationen über die Systeme oder angegliederte Systeme beschaffen. Außerdem kann ein Angreifer auf die entsprechenden Systeme zugreifen und dort die zuvor erwähnten Manipulationen vornehmen.

Zu (1.1): Die Adressstruktur der Netzwerke zeigt, in welchem Verhältnis die Server zueinander stehen, welche Abhängigkeiten bestehen und damit wie welche Systeme erreichbar sind und welche spezifischen Verwundbarkeiten durch schlechte Vernetzung entstehen.

Zu (1.2): Dieser Teil der Informationen ist wie bereits skizziert als der schädlichste und als gefährlicher anzusehen als der Verlust der Passwörter. Mit der Kenntnis der verwendeten Software, Hardware und der Betriebssysteme ist es einem Angreifer möglich, Verwundbarkeiten in den Strukturen der NATO zu identifizieren und folgend typische Schwächen auszunutzen. So ist etwa das häufig vorkommende Betriebssystem Solaris 10 ein kommerzielles, komplexes Betriebssystem, das zwar gute technische Security-Policies zulässt, andererseits aber selbst angreifbar ist, wobei in diesem System installierte Hintertüren als schlecht zu entdecken gelten. Bei einem professionellen nachrichtendienstlichen Angreifer etwa ist hier damit zu rechnen, dass bereits vorproduzierte Angriffe für Solaris 10 vorhanden sind, die der Angreifer bei Kenntnis des Vorhandenseins dieses Betriebssystems und bei einem Zugang sofort dort anbringen und folgend sicher verstecken kann. Bei einem größeren Nachrichtendienst wie etwa dem Russlands oder Chinas ist außerdem davon auszugehen, dass mehrere Angriffe auf Solaris 10 existieren und parallel verbaut werden, falls einer entdeckt werden sollte. Dies ist gängige nachrichtendienstliche Praxis.

Zu (1.3): Passwörter und IP-Adressen sind außerordentlich wertvoll, da hier eine erhebliche Zeitersparnis und Risikoreduktion bei der Anbringung von Angriffen zu gewinnen ist. Insbesondere Passwörter auf tieferen Systemebenen mit größeren Zugriffsrechten wie Root-Passwörter sind außerordentlich gewinnbringend. Mit diesen Passwörtern können eigene Zugänge gelegt werden, eigene Schadprogramme installiert werden und tiefere Systembetrachtungen vorgenommen werden, ohne dass

dabei hohe Risiken einer Entdeckung in Kauf genommen werden müssen. Dennoch sind Passwörter und IP-Adressen wandelbar und daher nicht so wertvoll wie die deutlich dauerhafteren Informationen über Software und Hardware, sofern dort eine ausreichende Zahl von Verwundbarkeiten anzunehmen ist. Im vorliegenden Fall spielen Passwörter und IP-Adressen vor allem eine wichtige Rolle, da sie es potentiellen Angreifern ermöglicht haben könnten, auch innerhalb eines kurzen Zeitfensters das gesamte NS-System der NATO unterwandert zu haben.

Zu (1.4): Zuständigkeiten für Server ergeben sich ebenfalls aus den Tabellen, wobei diese Zuständigkeiten, sofern aktuell, genutzt werden könnten, um weitere Zielpersonen zu identifizieren.

Zu (1.5): Die Informationen geben auch Einblick auf weitere technische und operative Details zum Aufbau der NATO NS-Netzwerke wie etwa die Strukturen des PAN-Netzwerkes oder die Procedere beim Aufbau der Server. Auch diese Informationen können strategisch genutzt werden.

Abschließend ist zu dieser Frage noch zu bemerken, dass der Begriff "vollständig" schwierig zu besetzen ist. Mit den vorhandenen Informationen erhält man ein sehr gutes Bild der betroffenen Systeme, das für einen Angreifer vorerst keine Fragen offen lässt, was aber nicht ausschließt, dass es doch noch relevante Informationen gibt, die nicht in den Informationen vorhanden waren.

4.2 *Lassen die in den Dateien enthaltenen Informationen allgemein Rückschlüsse auf die gesamte Computertopologie und -organisation der NATO zu und ggf. welcher Erkenntnisgewinn ergäbe sich hieraus für Akteure eines möglichen Cyber-Angriffs?*

Es ist einem Angreifer über Auswertung dieser Daten möglich, allgemeinere Rückschlüsse auf weitere Serverstrukturen der NATO zu ziehen wie etwa:

- wie die NATO allgemein Netzwerke aufbaut,

- welche Arten kommerzieller IT verbaut werden (Hardware und Software),

- wie gut und auf welche Weise strukturiert die Passwort- und Sicherheitskultur ist,

- wie IT-orientierte Arbeitsprozesse der NATO aussehen,

- wie viel Personal in welcher Qualität für IT und IT-Sicherheit eingesetzt wird,

- wie man Informationen aus anderen NS-Systemen exfiltrieren könnte.

Wie bereits oben erwähnt wurde, ist es als wahrscheinlich anzusehen, dass ein Angreifer mit den offenbarten Informationen weiter in die NATO-NS-Netzwerke eindringen und sich lateral dort bewegen konnte. Dabei ist primär die schlechte und generische Passwortkultur ursächlich, sekundär aber auch die Kenntnis der Vernetzungsformen und der verwandten Technologien. Da so auf viele weitere Systeme zugegriffen werden kann, ist der Erkenntnisgewinn und der erweiterte taktische Handlungsspielraum für einen Angreifer als hoch einzuschätzen.

4.3 *Welche Einwirkungsmöglichkeiten ergäben sich aus diesen Informationen für Anwender, die nur über das Internet, nicht jedoch über eine besondere Zugangsberechtigung zum NATO-Secret-System verfügen?*

Zu dieser Frage wurde oben Stellung genommen. Ein Angreifer, der keine Zugangsberechtigung hat, hat die folgenden Möglichkeiten:

- er kann das PAN-System von außen stören,

- er kann über fingierte Emails mit infizierten Dokumenten versuchen, in das NS-System zu gelangen und dort

-- ohne Rückkanal nur Störungen verursachen oder automatisierte Manipulationen installieren,

-- oder versuchen, einen Rückkanal aufzubauen, sofern er bestimmte Schwächen oder Mittel findet, die physische Grenzen zwischen PAN und NS zu überbrücken, wobei ihm folgend alle oben erwähnten Optionen für Operationen in den Zielsystemen zur Verfügung stünden.

4.4 *Welche Einwirkungsmöglichkeiten ergäben sich für Anwender mit Zugangsberechtigung zum NS-System?*

Bei Zugang zum NS-System, wie etwa über einen Innentäter, mit vollem Rückkanal, kann ein Angreifer alle oben erwähnten Operationen in hoher Qualität durchführen. Er kann spionieren, stören, sich lateral bewegen, sich gut tarnen, mehrere Hintertüren und automatisierte Angriffe legen, die kaum zu finden sein werden, alles Mögliche auf den Systemen anlegen und installieren und damit in jeder taktisch sinnvollen Form die Zielsysteme manipulieren, die dann immerhin das gesamte NS-Netz umfassen könnten.

4.5 *Setzen die in den Dateien enthaltenen Informationen einen kundigen Anwender in die Lage, einen sog. Trojaner in die Computersysteme der NATO einzuschleusen, um verschlüsselte Informationen aufzuspüren?*

Ja. Über die Root-Passwörter und Verwundbarkeiten in Hard- und Software könnte ein Angreifer eigene Schadsoftware einbringen, die bei hoher Tarnung spezifisch sensible und verschlüsselte Informationen sucht und exfiltriert. Dazu ist anzumerken, dass der in den Servertabellen vorhandene Hinweis "Encrypted pw" ein Hinweis auf Verschlüsselungsschlüssel sein kann. Dies ist aber eine offene Frage.

4.6 *Welche Einwirkungsmöglichkeiten ergäben sich aus den in den Dateien enthaltenen Informationen in Bezug auf Server, die mit der Funktion "NATO Security Script" gesichert sind?*

Auf diesen Punkt wurde oben bereits eingegangen. Auf Basis der vorliegenden Informationen stellt sich dies wie folgt dar: Die betroffenen Server könnten in jedem Fall gestört werden, es wären aber auch Zugänge auf die Daten und Funktionen der Server über die mit diesen Servern verbundenen, selbst aber nicht gesicherten Server möglich. Zudem bestehen noch Zweifel an der Funktionalität des NATO Security Script.

4.7 *Trifft es zu, dass mittels der in den Dateien enthaltenen Informationen nur Windows-basierte Server beeinflusst werden können?*

Nein, dies trifft nicht zu. Alle Server können beeinflusst werden. Auch die auf UNIX-basierenden Systeme sind verwundbar.

4.8 Im Folgenden wird noch - aus Zeitgründen nur knapp - auf die Fragen des Angeklagten eingegangen.

4.8.1 *Wie kann eine unbefugte Person außerhalb eines militärischen Areals Zugang zu den ICC-Servern erhalten?*

Hierfür wurden oben einige Beispiele skizziert. Es können Innentäter angeheuert werden, es kann von anderen Stellen des NS-Netzwerkes zugegriffen werden, es können Angriffe über das PAN-System eingeschleust werden, über die Supply Chain oder über Wechselmedien.

4.8.2 *Wie sind die Server physisch, hardware- und softwaremäßig gesichert?*

Hierzu finden sich in den Unterlagen kaum Hinweise. Die einzigen Sicherheitsmaßnahmen, die erwähnt werden, sind die physische Trennung NS-PAN, das NATO Security Script und die Passwörter. Diese Sicherheitsmaßnahmen sind alle eingehend besprochen worden. Sollte es sich bei diesen Sicherheitsmaßnahmen um alle vorhandenen Sicherheitsmaßnahmen des NS-Netzes handeln, wäre das Netzwerk nur schlecht gesichert.

4.8.3 *Wie sind die Passwörter der Dateien CCAI, P36ICC, CCAIR-NIRIS, IS NS NIRIS sowie project-02 in ihrer Sicherheitsstärke zu bewerten? Sind sie für geheime Systeme ausreichend?*

Wie bereits erwähnt wurde, sind die Passwörter herausragend schlecht und verstoßen gegen jede Regel. Passwörter dieser Art erhöhen deutlich die Unsicherheit. Sie sind für geheime Systeme nicht annähernd ausreichend. Sollten Folgeschäden für die NATO entstehen durch laterale Bewegung, ist die generische, schlechte Passwortkultur (inklusive der Idee, alle Passwörter zentral in Listen zu speichern) mit Schuld.

4.8.4 *Ist der Zweck der Passwörter ersichtlich, z.B. Benutzername?*

Ja. Bis auf wenige Ausnahmen sind die Passwörter generisch.

4.8.5 *Kann ein Benutzer geheime Daten, d.h. für einen begrenzten Personenkreis im DHS selbst zuverlässig geschützt abspeichern?*

Diese Frage kann ohne genauere Kenntnis des DHS nicht beantwortet werden. Der Vorfall demonstriert allerdings mindestens eine Instanz, dass dies nicht der Fall ist. Ob dieser Fall allerdings ein Ausreißer ist oder Indiz eines systematischen Fehlers, lässt sich nicht sagen.

4.8.6 Wie schwierig ist es, im DHS Dateien über "ICC", wie sie streitgegenständlich sind, zu finden?

Diese Frage kann ohne genauere Kenntnis des DHS nicht beantwortet werden. Der Vorfall demonstriert allerdings mindestens eine Instanz, dass dies möglich ist.

5. Zusammenfassung

Zusammenfassend lässt sich sagen, dass durch den Vorfall durchaus signifikanter Schaden entstanden ist.

Da das NS-System der NATO durchaus auf das Interesse einiger hochprofessioneller Nachrichtendienste mit sehr guten Vorbereitungen im Feld Cyber Warfare und Cyber Spionage trifft, wäre es durchaus möglich und plausibel, dass direkt nach dem Abfluss der Informationen im März 2012 ein Verkauf der Informationen stattgefunden hat. Folgend wäre es für diesen potentiellen Angreifer plausibel, möglichst schnell zu agieren und wie erwähnt weitere Zugänge und Angriffe zu legen, laterale Bewegungen zu unternehmen und ein hochwertiges und kaum zu detektierendes Darknet aufzubauen. So wäre der Angreifer unabhängig von möglichen Passwort- und Konfigurationsänderungen und hätte seine Investition in die Daten und einen dauerhaften strategischen Vorteil gesichert. Da die Erfahrung im Umgang mit solchen Angreifern wie bei vielen großen Spionagevorfällen der letzten Jahre klar gezeigt hat, dass solche Angreifer, wenn sie einmal tief in einem System sind, nicht mehr einfach detektiert und zuverlässig bereinigt werden können, wäre die aus Sicherheits- und Spionageabwehrperspektive jetzt notwendige Entscheidung, das gesamte NS-System vollständig neu aufzusetzen, und zwar zeitgleich, damit ein Angriff nicht ein neu aufgesetztes System durch eine Vernetzung mit einem infizierten System neu infizieren kann. Wie erwähnt muss hier allerdings der NATO und der äußerst schlechten Security Kultur eine Mitschuld attestiert werden, wenn es tatsächlich zu einer lateralen Ausbreitung eines Angreifers gekommen ist. Wären mehr und bessere Sicherheitsmechanismen in den Systemen, überhaupt sichere Systeme und nicht COTS-Produkte, wäre mehr hochqualifiziertes Personal und Geld für die IT-Sicherheit ausgegeben worden und wäre die Passwortkultur nicht so ungemein schlecht, hätte ein Angreifer nach Kenntnis der offenbarten Informationen erhebliche Schwierigkeiten und Risiken auf sich nehmen müssen, was vermutlich einen weit längeren Zeitraum und höhere Kosten bedeutet hätte und eine Ausbreitung in kritische Breite hätte verhindern können. Der Vorfall wäre dann begrenzt und zu beheben.

So ist dies allerdings nicht der Fall. Ein völliger und zeitgleicher Austausch wird aus operativen und finanziellen Gründen mit hoher Wahrscheinlichkeit nicht geschehen. Daher muss die NATO durch den Vorfall mit einer erhöhten Unsicherheit bezüglich der Zuverlässigkeit ihrer Systeme zurecht kommen. Dies wird der faktische strategische Schaden für die Gegenwart sein.

Eine echte Manipulation oder Spionagekapazität wird sich eventuell erst im Krisenfall bemerkbar machen. Dann könnte sie eine kritische Einschränkung bedeuten. Die Air Power der Alliance ebenso wie andere Fähigkeiten könnten kritisch behindert und modifiziert werden, wobei ein geschickter Akteur seine taktischen Aktivitäten auf diese Cyber Behinderungen exakt anpassen kann und so schnell einen

entscheidenden strategischen Vorteil hätte. Die Verteidigungsfähigkeit der Alliance wäre durch ein effizientes Darknet im NATO NS-System kritisch beeinträchtigt.

Neben dem gegenwärtigen strategischen Schaden der Unsicherheit und dem möglichen zukünftigen strategischen Schaden der kritischen Beeinträchtigung im Kriegsfall müssen einige der technischen Sicherheitsmaßnahmen zwingend erneuert werden. Passwörter und Netzwerkkonfigurationen sollten mindestens verändert werden. Die Kosten dieses Prozesses sind moderat.

77

Das Gutachten wurde am 29.8.2013 in Berlin fertiggestellt.

_____

Dr. Sandro Gaycken

Berlin, d. 29.8.2013

1. Ablichtung, 7 Seiten geheim

92

G E H E I M

Ergänzungen

zum Gutachten Strafsache KLAG

nach Vernehmung der Zeugen

Sachverständiger: Dr. Sandro Gaycken, Institut für Informatik, Freie Universität Berlin. Experte für Cyber Warfare, Cyber Defense, Cyber Spionage und allgemein Cyber Security.

Anschrift: Dr. Sandro Gaycken, Institut für Informatik, FU Berlin, Fabeckstraße 15, 14195 Berlin

Zuständige Kammer / Auftraggeber: Oberlandesgericht Koblenz, Staatsschutzsenat, Stresemannstraße 1, 56068 Koblenz

Datum der Abfassung: 25.9.2013

Beschreibung und Umfang: Diese Ergänzungen ergänzen das bereits gelieferte Gutachten zur beschriebenen Strafsache. Der Umfang beträgt 7 Seiten.

G E H E I M

- amtlich geheimgehalten -

Im Folgenden werden in einigen Punkten Ergänzungen zum Gutachten zur Strafsache KLAG abgegeben, die neue Informationen einbinden, welche nach Befragungen der Zeugen MULQUEEN, GOWIE und PETERS verfügbar waren.

1. Erreichbarkeit der betroffenen Systeme

Die im Gutachten getroffenen Aussagen zu diesem Punkt wurden grundlegend bestätigt. Nach Vernehmung der Zeugen können folgende Ergänzungen gemacht werden:

- Erreichbarkeit innerhalb des NS-Systems: Die im Gutachten bemerkten Sachstände sind grundlegend bestätigt und lassen sich wie folgt erweitern. Die betroffenen Systeme sind von jedem Punkt des NS-Systems aus erreichbar gewesen. Die NATO unternimmt zwar weitere Trennungen des NS-Netzes in ein WAN (Wide Area Network - ein großes Netzwerk) und mehrere LANs (Local Area Network - ein lokales Netzwerk), allerdings ist die Trennung zwischen diesen Systemen nicht physisch, sondern nach Angaben der Zeugen nur durch eine Firewall und eine erneute Passwortabfrage vollzogen. Firewalls sind nur als Schutzmaßnahmen gegen bekannte und gängige Bedrohungen zu erachten und entfalten gegen qualifizierte Innentäter keine Schutzwirkung. Die Passwörter dagegen könnten theoretisch eine geringe Schutzwirkung entfaltet haben, wenn Abfragen exklusiv und unumgehbar auf User-Passwörter abgezielt haben. Dies schien allerdings nicht der Fall zu sein. Bei Bekanntsein der Adressen der Server und der Admin- und Root-Passwörter könnte ein direkter Zugang möglich gewesen sein. Zudem könnte ein Angreifer das User-Passworter von KLAG genutzt haben. Ob dies der Fall ist, lässt sich nicht nachvollziehen, da (a) keine Log-Dateien über User-Aktivitäten geführt werden und da (b) auch keine forensische Untersuchung nach dem Fall unternommen wurde.

- Erreichbarkeit weiterer Systeme über die kompromittierten Systeme: Von den betroffenen Systemen aus könnten sich Angreifer weiter in das NS-Netz bewegt haben, indem sie die betroffenen Systeme als Basis für weitere Operationen genutzt haben. Dieser Sachstand wurde bereits im Gutachten erwähnt.

- Erreichbarkeit von Außen: Die im Gutachten geäußerten Sachstände haben sich hier nicht geändert.

Die Kenntnisse sind so bereits grundlegend im Gutachten geäußert. Dort wurde bereits vorgebracht, dass die betroffenen Systeme ohne Probleme innerhalb des NS-Netzes erreichbar sind und unter einigem Aufwand ebenso von Außen.

2. NATO Security Script und weitere technischen Schutzmaßnahmen

Die im Gutachten getroffenen Aussagen zu diesem Punkt wurden grundlegend bestätigt. Die Funktionsweise des NATO Security Scripts stellt sich nach Vernehmung der Zeugen genauer wie folgt dar:

- Das NATO Security Script kann eine Fern-Anmeldung auf Root- oder Admin-Niveau auf den betroffenen Systemen über das NS-Netzwerk verhindern. Entsprechende Anfragen werden nach Angaben der Zeugen

nicht zugelassen. Eine Nutzung der Root-Passwörter wäre damit (bei fehlerfreiem Funktionieren des NATO Security Scripts, was weiterhin nicht vorausgesetzt werden kann) nur noch durch einen physischen Reboot des Systems vor Ort möglich. Dies ist allerdings nach Aussagen der Zeugen taktisch nicht möglich, da ein solcher Reboot etwa 40 Minuten dauert, aber nach zwei Minuten bemerkt wird, wonach nach weiteren fünf Minuten Personal im Serverraum wäre.

- Trotzdem muss das NATO Security Script für den vorliegenden Fall als irrelevant erachtet werden. Wie insbesondere der Zeuge Peters aussagte, hatten mehrere der betroffenen Systeme während der Phase der möglichen Exposition im Sommer 2012 Kompatibilitätsprobleme zwischen Funktionen wie JChat und dem NATO Security Script. Das NATO Security Script verhinderte das Funktionieren missionskritischer Software. Daher war das NATO Security Script auf mehreren aktiven und kritischen Servern NICHT AKTIVIERT. Damit wird es jedem Angreifer während des Zeitraum zwischen dem ersten Entwenden der Informationen durch KLAG und der Behebung der Schwachstellen ohne Probleme und Widerstände möglich gewesen sein, von jedem Punkt des NS-Netzwerkes und unter den im Gutachten geschilderten Bedingungen auch von Außen auf die Server bis auf Root-Level zuzugreifen.

3. Verbindung zu Top Secret Daten

Als neuartig und in besonderem Maße besorgniserregend muss aus den Vernehmungen festgehalten werden, dass die betroffenen NS-Systeme auch den physischen Backbone der Top Secret Systeme bilden. Top Secret Daten sind also physisch ebenfalls im als kompromittiert zu erachtenden NS-System gelagert und darüber erreichbar. Laut der Zeugen sind weitere Sicherheitsmaßnahmen vorhanden, die die Top Secret Abschnitte im NS-Netzwerk schützen, es müssen allerdings Zweifel an der Funktionalität dieser Sicherheitsmaßnahmen gegenüber nachrichtendienstlichen Angreifern angemeldet werden. Einer der Zeugen benannte eine Sicherheitsmaßnahme, die bereits als hintergehbar bewertet werden muss.

Durch die mögliche Kompromittierung des NS-Netzwerkes ist also auch von einer möglichen Kompromittierung der Top Secret Informationen der NATO auszugehen, für alle Daten, die das NS-System als Backbone genutzt haben.

Dies muss als besonders bedenkenswert erachtet werden, da mit diesen Informationen der NATO und ihren Mitgliedern und Partnern erheblicher strategischer Schaden entstehen kann. Zudem basieren die auf den Top Secret entstehenden und ebenfalls entsprechend klassifizierten Top Secret Beschlüsse zumeist auf umständlichen und langwierigen, oft monate- bis jahrelangen Abstimmungsverfahren zwischen den Mitgliedern, die sich in angemessener Zeit in ihrer Gesamtheit nicht erneut durchführen lassen. Die strategische Planung ist damit nicht nur kurzfristig, sondern in den meisten Bereichen überaus langfristig und nachhaltig potentiell unterwandert und damit nicht mehr vertrauenswürdig und gestört.

4. Passwort-Policy

In diesem Kontext sind die grundlegenden Beobachtungen des Gutachtens nach wie vor zutreffend. Folgende Ergänzungen lassen sich machen:

- User-Passwörter der einzelnen Nutzer sollten den erforderlichen und vorgeschriebenen Sicherheitsmerkmalen genügen und eine hohe Komplexität aufweisen.

- Auch andere Passwörter sollten diesen Sicherheitsmerkmalen theoretisch genügen. Hierbei besteht allerdings die operative Schwierigkeit, dass komplexe und individuelle Passwörter (a) eine längere Zeit für die Eingabe erforderlich machen und (b) das Führen einer Passwortliste erfordern, die im Falle einer Nutzung eines Passwortes verfügbar und schnell einsehbar sein muss. Die Bedingungen (a) und (b) führen laut der Zeugen insgesamt zu einem Zeitaufwand von einigen Minuten, der im Falle eines Rechnerzusammenbruchs im Kontext einer Reaktion etwa auf einen Raketenangriff eine zeitgemäße militärische Reaktion unmöglich macht. Die Sicherheitsstrukturen der NATO machen folglich auf Administratoren- und Root-Level kurze, einfache und universale Passwörter operativ erforderlich. Daher hat sich die praktische Passwortkultur auch nach dem Vorfall nicht wesentlich geändert. Die Schutzwirkung der Passwörter muss damit als insgesamt ungenügend, das Sicherheitskonzept als strukturell und dauerhaft fehlerhaft bewertet werden.

5. Erlangen und Unterwandern von NATO-spezifischer Software über die betroffenen Rechnerstrukturen

In diesem Punkt sind erneut keine grundlegenden Änderungen des Gutachten vorzunehmen. Folgende Ergänzungen lassen sich machen: Die Vernehmungen der Zeugen haben ergeben, dass es prinzipiell möglich wäre, über einen Zugang zu den Rechnerstrukturen auch NATO-spezifische Software zu besorgen. Es sind etwa Installationsdateien auf verschiedenen Rechner vorhanden, um Desktop-Installationen vornehmen zu können. Auch ein Reverse Engineering der installierten Software wäre möglich. Dies ist wie im Gutachten erwähnt besonders besorgniserregend, da damit die Integrität dieser Software systemweit nicht länger als gewährleistet gelten kann. Ein potentieller Angreifer könnte die Software besorgt und auf Schwachstellen getestet haben, von denen sich in der Regel mehrere Tausend in entsprechenden Programmen befinden, insbesondere bei Eigenentwicklungen wie in diesem Fall. Diese Schwachstellen sind im Regelfall noch auf einige Jahre ausbeutbar, Zugriffe und Manipulationen praktisch nicht erkennbar. Eine Integrität der Software (JChat, NIRIS, FAST, ICC, NATO Security Script) lässt sich nur herstellen, indem eine vollkommen neuartige Software entwickelt und implementiert wird. Die Software JChat, NIRIS, ICC und FAST wurde von den Zeugen als überaus missionskritisch bewertet.

6. Weitere Bemerkungen zur IT-Sicherheitskultur der NATO

In Ergänzung zum Gutachten kann festgehalten werden, dass die IT-Sicherheitskultur der NATO technisch und operativ nicht nur in Bezug auf Passwörter, sondern insgesamt bemerkenswert schlecht ist. Die Vernehmung der Zeugen hat hier die folgenden neuen Sachstände eröffnet:

- Innerhalb des NS-Netzwerkes gibt es abgesehen von dem scheinbar nicht konsequent verwendeten NATO Security Script, der Firewalls und Passwortabfragen zwischen WAN und den LANs keine weiteren

Sicherheitsmaßnahmen. Für einzelne Folder und Drives werden Rechte über "Security Groups" vergeben, die über die "Core Services" determiniert werden. Dies ist eine sehr rudimentäre Form der Sicherung, die insbesondere gegen qualifizierte Innentäter kaum Schutzwirkungen entfaltet. Für den vorliegenden Fall ist davon auszugehen, dass diese Sicherheitsmechanismen nicht besonders effizient sind . Zur Frage der Innentäter-Abwehr äußerte einer der Zeugen, dass das wesentliche Konzept dazu die Sicherheitsüberprüfung sei. Bei einem System mit (nach Zeugenaussagen) 70.000 bis 80.000 Nutzern ist dies als zentrale Annahme als naiv und ungerechfertigt zurückzuweisen.

- Zur Sicherung geheimer Dokumente wurde von den Zeugen ausgedrückt, dass hier das wesentliche Konzept die korrekte Ablage in den korrekten Foldern auf den korrekten Kompartmentalisierungen ist. Die Möglichkeit der Angabe von Freigaben in den Metadaten war nicht allen Zeugen bekannt und scheint vom System nicht durchgesetzt zu werden. Die einzige weitere Sicherheitsmaßgabe ist ein "SECRET"-Vermerk auf dem Dokument selbst, der aber natürlich leicht entfernt werden kann. Damit kann insbesondere eine unqualifizierte Migration von Geheimdokumenten im NS-System nicht verhindert werden. Die Zugänglichkeit von Innen hängt am korrekten Gebrauch durch die Mitarbeiter, die Core Services sowie am korrekten Funktionieren der Systeme. Das korrekte Funktionieren der Systeme kann nach dem Vorfall NS-weit nicht mehr als gewährleistet gelten, so dass also in Abwesenheit weiterer Schutzkonzepte eine mögliche dauerhafte Kompromittierung geheimen Materials stattgefunden hat.

- Die Integrated Solaris Platform (ISP) ist ein kommerzielles Off-The-Shelf Produkt und vorrangiges Betriebssystem der NATO Serverstrukturen, das in der NATO durchgängig genutzt wird in einer Variation, die einige besonders offene Schwachstellen strukturell umgangen oder abgeschaltet hat. Diese leicht besser gesicherte Plattform wird von der NATO als "NISP" bezeichnet (NATO-ISP). Bei der Verbesserung ist nicht davon auszugehen, dass diese ein angemessenes Niveau gegen nachrichtendienstliche Angreifer anstrebt oder erreichen kann. Für den vorliegenden Fall entfaltet also auch dieser Schritt keine Sicherheitswirkung.

7. Verdächtige Tabellen

Neu in Ergänzung zum Gutachten kann bemerkt werden, dass die Tabellen mit den Nachweisen der physischen Orte und der logischen Adressen der Server als verdächtig einzustufen sind. Die Zeugen haben hier angegeben, dass sie ihre Server gut genug kennen, um solche Tabellen nicht zu benötigen, während andere Personen außerhalb der entsprechend zuständigen Abteilungen diese Tabellen nicht benötigen würden. Diese Aussagen sind überaus plausibel, so dass angenommen werden könnte, dass der KLAG diese Listen extra angelegt hat. Die Listen wären vorrangig und hervorragend für Innentäter nutzbar.

7. Entfaltung schädlicher Wirkungen

In diesem Punkt wurden die Sachstände des Gutachtens nicht berührt. Die Zeugen haben bestätigt, dass durch die offengelegten Materialien alle Strukturen offen zugänglich waren und dass ein Angreifer damit

auf alle Systemfunktionen, alle Daten, jede Software und auf das gesamte weitere NS-Netzwerk zugreifen konnte. Wie im Gutachten erwähnt, hätte das genutzt werden können, um weiteren Zugriff, weitere Infektion durch laterale Bewegungen und schlussendlich Spionage und Sabotage an beliebigen Stellen des NS-Systems durchzuführen. In Ergänzung lässt sich noch anbringen:

- Potentielle Gegner können über den Zugriff auf das NS-System auch Zugriff auf Beschlüsss, auf Verfahren und auf Methoden der NATO erhalten. In den betroffenen Systemen betrifft dies etwa das marine und das Luftlagebild und das Command & Control der Luft- und Seestreitkräfte sowie die Raketenabwehrsysteme der NATO, wobei aber mittelbar auch von einer Betroffenheit aller weiteren Systeme und Daten auszugehen ist. Beschlüsse sind oft über alle Mitglieder zu treffen und lassen sich bei Kompromittierung nicht widerholen. Planungen und Verfahren haben zudem zahlreiche operative und technische Ausprägungen mit erheblichen systemischen Abhängigkeiten zur Folge, so dass auch hier nach der Kompromittierung kein einfacher "Reset" auf einen neuen und wieder sicheren Zustand möglich ist. Der Vorfall macht somit allein durch die Möglichkeit der Unterwanderung eine vollständige Erneuerung nicht nur der technischen Strukturen, sondern auch vieler Beschlüsse und Verfahren erforderlich, was aber erneut rein pragmatisch als unmöglich betrachtet werden muss und so also in einer weiteren Dimension die NATO in Zukunft hoher Entscheidungsunsicherheit aussetzt.

- Diese Entscheidungsunsicherheit kann bereits im aktuellen Syrienkonflikt operativ relevant sein. Es ist als möglich zu erachten, dass der syrische Dienst für Electronic Warfare über den Vorfall an Daten gelangt ist, die Operationen der NATO in Syrien unmöglich machen.

- Als weiteres Detail lässt sich ergänzen, dass über die Informationen zum System SOCC-LINC-E8 eine Manipulation der WAN GUIs des NS-System möglich gemacht wurde, da auf dieser Datei offenbart wurde, dass auch für dieses System generische Passwörter verwendet werden. Das WAN GUI erlaubt eine Fern-Verwaltung von taktischen Informationen durch das NS-Netz. Mit dem Passwort ließe sich etwa steuern, welcher Teil des NS-Netzwerkes welche Informationen zu welchem Zeitpunkt bekommt oder nicht bekommt. Damit könnte eine Führung der betroffenen Truppenteile nachhaltig verhindert oder sogar in eine Gefahrensituation gebracht werden.

Damit können für die Ergänzungen folgende abschließende Bemerkungen getroffen werden:

Die Grundaussagen des Gutachtens sind durch die Zeugenaussagen nicht betroffen und grundlegend bestätigt. Übergreifend müssen die Zugriffsmöglichkeiten, der Zeitraum und die Zugriffstiefen nach wie vor als vollkommen ausreichend erachtet werden, um von einer Kompromittierung des gesamten NS-Systems auszugehen. Dabei ist weiterhin davon auszugehen, dass viele der Sicherheitsmaßnahmen leicht umgangen werden können, so dass also die laterale Bewegungen eines möglichen Angreifers kaum erschwert gewesen sein könnte. Es ist also weiterhin als möglich zu erachten, dass das System systemweit und im Weiteren unerkennbar unterwandert und damit nicht länger vertrauenswürdig ist. Zudem ist es nicht unwahrscheinlich, dass ein Angreifer Zugang zu dem System hatte und eine Kompromittierung vornehmen konnte. Sollte der KLAG tatsächlich einen Verkauf der Daten beabsichtigt haben, wäre bereits die Abgabe einer einzigen Datei mit einem irgendwie aktiven Gerät - ob operativ, im

Testbetrieb oder im Build -, um potentiellen Käufern eine Zugriffsmöglichkeit real beweisen zu können, als prinzipiell ausreichender Vektor zu erachten. Ein vollständiger erfolgter Verkauf der Daten hätte hier noch eine wesentliche Erleichterung und Verbreiterung gegnerischer Aktivitäten ermöglicht. Zudem ist es unter offensiven Cyberspionen üblich, bei einem einmal erfolgreichen Zugriff, den Zugang maximal auszubauen und nachhaltig zu sichern. Dies sind in der Regel die ersten Aktivitäten eines qualifizierten Angreifers. Auch bei nur einem minimalen Abhandenkommen der Daten kann also eine sehr weit reichende und nicht mehr zu detektierende Infektion als wahrscheinlich angenommen werden. Wie im Gutachten berichtet wurde, genügte hier bereits das Versenden via GMX als hinreichende Öffnung, wobei das folgende Zeitfenster bis zum Ergreifen der Gegenmaßnahmen mehr als ausreichend gewesen wäre, um eine Reihe von Operationen durchzuführen, zu testen und dauerhaft zu konsolidieren.

Der Schaden für die NATO ist wie im Gutachten erwähnt auf verschiedenen Ebenen zu sehen. Technisch wäre nach wie vor wie zuvor genannt eine vollständige und zeitgleiche Erneuerung der Systeme notwendig, wobei ein Teil neu aufgesetzt werden müsste, während Betriebssysteme und Software neu ausgewählt, beziehungsweise neu entwickelt werden müssten. Da dies praktisch unmöglich ist, muss die NATO folgend mit einer hohen Entscheidungsunsicherheit leben, die bereits im aktuellen Syrienkonflikt operativ relevant sein könnte, da in diesem Fall ein Cyber-interessierter Nachrichtendienst vorhanden wäre, dem eine unbekannte Kooperation mit einem an einem Ankauf der Informationen sehr interessierten Nachrichtendienst wie dem russischen FSB unterstellt werden kann.

Eine Integrität der Systeme und damit ein Gelingen von Führung und Kommunikation kann nicht mehr gewährleistet werden.

98

Herrn
Bundesanwalt beim BGH Dietrich
zzt. OLG Koblenz

VS-Empfangsschein

Anlage(n)

Geschäftszeichen (Aktenzeichen und Vs-Bestands- bzw. Tagebuchnummer)	Datum	Anzahl	Aufs.-Nr. (Nur bei GEHEIM/STRENG GEHEIM)
3 StE 1/13-2 Tgb.-Nr. 1/13 VS-geheim	7.10.13	1	1. Ausfertigung des Gutachtens Dr. Gaycken vom 25.9.2013

SOFORT
offen zurück an:

Oberlandesgericht Koblenz
Stresemannstraße 1
56068 Koblenz

Empfangen am 7. 10. 2013

Unterschrift