Der Netzwerk Insider

Systematische Weiterbildung für Netzwerk- und IT-Professionals

# IT-Sicherheit im Zeitalter der Cyberangriffe

**von Dr. Melanie Winkler**

Dr. Melanie Winkler ist als Beraterin bei der ComConsult Beratung und Planung GmbH in dem Bereich IT-Sicherheit tätig. Dort beschäftigt sie sich besonders mit Sicherheitskonzeptionen nach ISO 27001 und BSI Grundschutz und deren Umsetzung.

**Jedem Nutzer elektronischer Daten sollte mittlerweile klar geworden sein, dass alle Informationen, welche über ein öffentliches Netz übertragen werden, generell durch Unbefugte abgegriffen werden können. Dies gilt umso mehr seit den Enthüllungen durch Edward Snowden und die dadurch öffentlich bekannt gewordenen Angriffe auf vertrauliche Daten unterschiedlicher Art durch große Hackerangriffe. Daher wird natürlich schon seit einiger Zeit, zum Beispiel durch das BSI, die Empfehlung ausgesprochen, vertrauliche Daten ausschließlich verschlüsselt zu übertragen und zu speichern.**

Im Rahmen der Enthüllungen durch Edward Snowden ist jedoch auch bekannt geworden, dass zumindest einige große Hackergruppen - häufig mit staatlicher Unterstützung - über weitere Methoden verfügen, an Informationen zu gelangen, welche für sie von Interesse sind. Es stellt sich Unternehmen und Privatanwender daher immer mehr die Frage, wie sicher ihre Daten wirklich noch sind. Lohnt es sich beispielsweise als Endanwender überhaupt noch Daten zu verschlüsseln oder können diese nicht sowieso mit vergleichbar geringem Aufwand entschlüsselt und gelesen werden?

In diesem Artikel werden die wesentlichen der aktuell bekannten Gefährdungen dargestellt und es wird aufgezeigt, wie man sich zumindest gegen einige dieser Bedrohungen schützen kann und welche Grenzen hier aktuell bestehen.

## 1.1 Zugriff auf Daten

### 1.1.1 Zugriff durch Abfangen von Daten

In vielen Fällen durchlaufen Daten zu einem Zeitpunkt während ihrer Übertragung ein öffentliches Netz und können dann von einem Angreifer an einem Punkt der Verbindung abgefangen und ausgewertet werden. Werden die Informationen unverschlüsselt übertragen, so können diese direkt vom Angreifer abgehört oder umgeleitet, gespeichert und genutzt werden. Ein Abfangen übertragener Daten ist in allen Bereichen von Kommunikationsverbindungen möglich.

Beispielsweise werden bei jedem normalen Telefonat Daten über ein öffentliches Netz übertragen. Dabei handelt es sich hauptsächlich um Sprachdaten, welche zwischen den Teilnehmern ausgetauscht werden sollen. Bei Telefonaten werden die Sprachdaten normalerweise (zumindest auf Teilen der Gesamtübertragungsstrecke) unverschlüsselt übertragen. Das bedeutet, dass ein Angreifer, welcher die Leitung abhört oder ein Gespräch mitschneidet, dieses unmittelbar verstehen kann.

Auch für Informationen, welche über das Internet verschickt werden, ist es möglich, diese mit geeigneten Werkzeugen abzufangen. Dies ist beispielsweise gegeben, wenn per E-Mail kommuniziert wird

# Der Netzwerk Insider

## Systematische Weiterbildung für Netzwerk- und IT-Professionals

oder im Internet Daten ausgetauscht werden. Es werden aber auch Daten übers Internet übertragen, wenn ein Mitarbeiter von außerhalb des Büros auf ein Firmennetz zugreift (VPN Zugriff) oder einen Rechner von Extern administriert (Zugriff über SSH).

Darüber hinaus kann auch auf Daten zugegriffen werden, welche lediglich auf dem System gespeichert sind, aber nicht über das Netz übertragen werden. Ein solcher Zugriff ist dann durchführbar, wenn über Schadsoftware, Sicherheitslücken oder sogenannte Backdoors auf ein System und die darauf befindlichen Daten zugegriffen werden kann. Außerdem existiert auch Schadsoftware, welche Daten des Systems direkt an einen Angreifer überträgt. Ein Beispiel für eine solche Schadsoftware ist „EquationDrug“. Mit Hilfe dieser Software können die Personen, welche die Software auf den Rechner eingeschleust haben, Daten vom Rechner abziehen. Sie können so beispielsweise Informationen darüber erhalten, was auf der Tastatur getippt wird oder welche Seiten im Browser geöffnet wurden.

Die hier beschriebenen Zugriffe auf Informationen sind jedoch bei immer weiter steigenden Datenmengen sehr mühsam. Die Größenordnung sowohl der gespeicherten Daten, als auch der übertragenen Daten steigen von Tag zu Tag. Daher sind derartige Vorgehensweisen des Abfangens sehr aufwendig und erfordern einen hohen Einsatz an Zeit und Ressourcen zur Speicherung und Auswertung der abgefangenen Daten.

### 1.1.2 Gezielte Angriffe auf Systeme

In der Vergangenheit ist es bereits vorgekommen, dass Certificate Authorities, welche die privaten SSL Schlüssel vieler bekannter Hersteller verwalten, durch externe Angreifer attackiert und dabei private Schlüssel gestohlen wurden. Somit ist jede SSL Kommunikation, welche mit den zugehörigen öffentlichen Schlüsseln kodiert wurde, ohne viel Aufwand mit den gestohlenen privaten Schlüssel in Echtzeit zu entziffern. Eine andere Methode verschlüsselte Kommunikation zu entschlüsseln benötigt Eingriffe auf die kommunizierenden Komponenten.

Angriffe auf solche Komponenten zielen beispielsweise darauf ab, die Konfigurationen der Verschlüsselung zu modifizieren. Dabei kann eine Verschlüsselungsart eingestellt werden, die der Angreifer ohne privaten Schlüssel entschlüsseln kann. Solche Modifikationen können an den Konfigurationen der E-Mail Clients, Router oder VPN-Clients vorgenommen werden. Daher gehören Benachrichtigungen und Logging im Falle von Konfigurationsänderungen an Software und Hardware zu wichtigen Sicherheitsfeatures.

Die Angriffe auf Endpunkte sind jedoch wesentlich aufwendiger als Eingriffe in die Kommunikation. Viele der bekannten Angriffe auf Endpunkte benötigen physikalischen Zugriff zum Endpunkt (z.B. USB-Stick in Laptop einschieben). Solche Angriffe können jedoch auch über Backdoors in auf dem Endpunkt installierten Programmen initiiert werden, z.B. durch böswillige E-Mail Anhänge und modifizierte Update-Pakete für das Betriebssystem oder einzelne Programme.

Eine weitere Methode gezielt auf Daten zuzugreifen ist heutzutage weit verbreitet. Sie wird „Advanced Persistent Threat“ (APT) genannt. Ein APT besteht meist aus mehreren aufeinander abgestimmten Angriffsformen und verfolgt ein festumrissenes Angriffsziel (z.B. Industriespionage).

Ein APT lässt sich in 5 verschiedene Phasen unterteilen:

1. Auskundschaften / Zielerfassung:
   Bevor ein erster Angriff auf das System erfolgt, informiert sich der Angreifer möglichst genau über den Aufbewahrungsort (z.B. Server, Rechenzentrum, Laufwerk, …) der Daten. Hierzu kann er sowohl auf öffentlich zugängliche Informationen zugreifen (z.B. eine unsicher konfigurierte Fehlermeldungswebseite eines Apache Servers) als auch gezielt Informationen erfragen (Social Engineering, Spear Phishing, …).

2. Eindringen und Erstinfektion:
   Nachdem der Angreifer die gesuchten Informationen grob lokalisiert hat, versucht er gezielt an diese heranzukommen. Ziel dieser Phase ist es als Vorbereitung für einen Zugriff auf die gewünschten Daten, unentdeckt in das System einzudringen. Dies erfolgt beispielsweise darüber, dass im ersten Schritt auf dem Zielsystem installierter Schadcode gezielt weitere Software auf dem System installiert. Bei dieser handelt es sich häufig um einen speziellen Trojaner, der oft ironisch als Remote Administration Tool (RAT) bezeichnet wird und welcher mit dem Command and Control Server (C&C) kommuniziert.

# Der Netzwerk Insider

Systematische Weiterbildung für Netzwerk- und IT-Professionals

3. Folgeinfektion (en):
   Sollte der Angreifer nach der Erstinfektion noch nicht auf alle für ihn wünschenswerten Daten zugreifen können, dann wird er von seinem ersten Einfallstor aus weitere Systeme infizieren. Dieser Schritt ist häufig wesentlich leichter als die Phase der Erstinfektion, da die Sicherheit nach Außen bei den meisten Systemen wesentlich besser ist als die interne Sicherheit. Dieser Schritt ist auch notwendig, wenn im ersten Schritt zwar eine Infektion eines Systems im Zielnetzwerk (z.B. ein normaler PC), aber keine direkte Infektion des Zielsystems (z.B. Administrations-PC, Server…) möglich war.

4. Datendiebstahl / Sabotage:
   In dieser Phase beginnt die Übertragung interessanter Daten in großen Mengen. Bis zu dieser Phase hat der Eindringling noch keine Daten abgegriffen und keine großen Datenmengen kopiert, um nicht aufzufallen. Diese Phase birgt das größte Risiko entdeckt zu werden, da hier Anomalien in Bezug auf den Datenverkehr und die durchzuführenden Aktionen (Datenbank-Dump, Kopieren von Dateien, …) gemessen werden können. Nach Abschluss dieser Phase hat der Angreifer die gewünschten Daten abgegriffen und der Schaden ist vollständig verursacht.

5. Verwischen von Spuren:
   Sollte der Angriff nicht aufgefallen und unmittelbar blockiert worden sein, so hat der Angreifer noch die Möglichkeit Spuren zu verwischen. Hierzu gehört das Löschen von Log-Dateien, Verbindungsinformationen und des Terminalverlaufs. Außerdem löscht sich die Schadsoftware selbst oder sie löscht einen Teil von sich und wird inaktiv. Wird diese Phase ebenfalls erfolgreich abgeschlossen, so fällt es den Geschädigten wesentlich schwerer den Angreifer und das Ausmaß des Schadens zu bemessen.

#### 1.1.3 Zugriff auf rechtlichem Wege

Ein wesentlich angenehmerer und weniger aufwendigerer Weg an Informationen zu gelangen, ist mit der Unterstützung der Informationshalter. Wenn also Hersteller dazu gebracht werden können, Zugang zu ihrer Software / Firmware bereitzustellen, dann spart dies Zeit gegenüber der Informationsbeschaffung durch Angreifer. Außerdem können die Grenzen, die durch andere Beschaffungsmöglichkeiten vorhanden sind, gegebenenfalls aufgehoben werden. So muss beispielsweise bei einem Abtransport von großen Datenmengen durch die Angreifer nicht vermieden werden, dass der Datenfluss auf Ebene des Netzwerkverkehrs auffällt.

Eine Grundlage für einen solchen rechtlich legitimen Zugriff auf sensible Informationen bietet den Geheimdiensten der USA der Foreign Intelligence Surveillance Act (FISA). Dieses Gesetz regelt insbesondere Fragen zur Auslandsaufklärung und Spionageabwehr. Es beschreibt unter anderem, dass Informationen von verdächtigen Personen, die bestimmten Kriterien entsprechen, für die Regierung der Vereinigten Staaten von Amerika zugänglich gemacht werden müssen. Zu diesen Kriterien gehören beispielsweise, dass die Person kein US-Bürger ist und sich nicht auf dem Territorium der USA aufhält. Jedoch können unter bestimmten weiteren Auflagen auch US-Bürger mit dem FISA durchleuchtet werden.

Laut amerikanischer Rechtsprechung unterliegen dem FISA alle auf amerikanischem Boden agierenden Unternehmen. Hierzu gehören unter anderem Microsoft, Yahoo, Google, Facebook, AOL, Skype, YouTube und Apple. Somit kann beispielsweise bei einem terroristischen Verdacht auf rechtlichem Wege Einsicht in die E-Mail-Konten von verdächtigen Personen erlangt werden.

Um solche Informationen von den betroffenen und interessanten Unternehmen zu erhalten, gab es laut den Dokumenten von Edward Snowden mehrere Treffen zwischen Regierungsvertretern (NSA, CIA, FBA, …) und Vertretern der Unternehmen (inklusive CEOs). Diese Treffen wurden unter der Enduring Security Framework (ESF) Initiative abgehalten. Dabei wurden angeblich sowohl die Art der benötigten Informationen, als auch die Übermittlungswege für Daten besprochen.

Aber nicht nur amerikanische Geheimdienste und damit auch die amerikanische Regierung können auf diesem Weg an Informationen gelangen. Durch Weitergabe können die so erlangten Informationen auch von anderen Geheimdiensten und Regierungen genutzt werden, welche mit der USA zusammenarbeiten. Laut den Dokumenten von Edward Snowden muss mindestens mit einer Weitergabe an die Geheimdienste und Regierungen verbündeter Staaten der USA gerechnet werden. Allerdings ist auch zu beachten, dass es sich hierbei um einen sehr speziellen Weg der Informationsgewinnung handelt. Auf diese Art Informationen zu erlangen können zwar einige der Geheimdienste zurückgreifen, jedoch außerhalb dieser Kreise ist dies nicht möglich. Maßnahmen zu ergreifen, welche gegen diese Art von Angriff nicht schützen können, sind daher trotzdem sinnvoll, um sich vor sonstigen Hackerangriffen zu schützen.

Die Art der Informationen, welche über diesen Weg erlangt werden können, hängen vom jeweiligen Anwendungsfall und von der ausgespähten Applikation ab. So wird in manchen Veröffentlichungen behauptet, die abgegriffenen Informationen würden sich auf Metadaten beschränken. Diese Datensätze beinhalten beispielsweise Informationen darüber, wer mit wem, wann und wie lange kommuniziert hat. Andere Veröffentlichungen beschreiben jedoch die Übertragung vollständiger Datensätze, also auch die Inhalte von E-Mails, Facebook-Profilen, Skype-Kommunikationen und Kalendereinträgen.

Die Wege über welche ein Angreifer an Informationen gelangen kann, hängen von den Applikationen und Szenarien ab. Im Folgenden geben wir einen Überblick.

### 1.2 Übertragungswege von Daten

Für die Übertagungswege von Informationen an unberechtigte Dritte gibt es unterschiedliche Möglichkeiten. Zum einen ist eine Übertragung über bestehende Sicherheitslücken und einen darüber erfolgenden Datenabgriff möglich. Andererseits können auch Daten auf unterschiedlichen Ebenen (siehe dazu auch Abbildung 1) bewusst übertragen werden. Dies beinhaltet auch einen Vollzugriff für bestimmte Parteien auf alle Daten eines

# Der Netzwerk Insider

## Systematische Weiterbildung für Netzwerk- und IT-Professionals

Unternehmens. Ein wissentlich (z.B. unter dem FISA) genehmigter Vollzugriff auf alle Informationen wird allerdings bisher von keinem Unternehmen zugegeben.

- **Applikationsebene**
  Auf Applikationsebene werden Datensätze aus Anwendungen wie Facebook oder Google explizit beim Unternehmen angefragt. Falls diese Anfragen akzeptiert und Daten an den Antragsteller übermittelt werden, so verwendet man für die Übergabe der Informationen dafür definierte Prozesse.

  In diesen Prozessen spielen Übergabeportale eine entscheidende Rolle. Das Unternehmen stellt die von der Regierung angefragten Datensätze in einem solchen Portal (beispielsweise eine Anwendung oder Webseite) zur Verfügung. Zugriff auf das Portal hat ausschließlich der Antragsteller (z.B. ein Regierungsvertreter). Nachdem die Daten von dem Antragsteller eingesehen (und ggf. kopiert) wurden, werden diese aus dem Portal gelöscht.

  Weitere Dokumente beschreiben eine andere Art der Informationsbeschaffung. Hierbei platzieren Regierungsvertreter unter Absprache mit den Unternehmen Personal in den Räumlichkeiten des Unternehmens mit entsprechenden Zugriffsrechten. Diese Personen können dann die Anfragen seitens der Regierung vor Ort abarbeiten.

  The Guardian beschreibt, dass die Zugriffe der NSA auf Microsoft Freemail-Dienste wie beispielsweise Outlook vor der Verschlüsselung der Inhalte geschehen. Auch auf die verschlüsselten Chats über Outlook.com hat die NSA seitens Microsoft Zugriff. Und seitdem Microsoft Skype gekauft hat, wird angeblich nicht mehr nur das Audio-Signal aufgenommen, sondern auch Video. Skype hat weltweit ca. 660 Mio. Nutzer. Daher gehen Kritiker davon aus, dass Microsoft mit Updates für seine Software und Services auch neue Instrumente ausliefert, um auch zukünftig den Anforderungen seitens Gesetzgeber gerecht werden.

  Weiterhin ist auch eine Ausnutzung von Schwachstellen auf Applikationsebene möglich. So kann ein Angreifer über Fehler in der Implementierung auf Daten zugreifen, welche von der jeweiligen Applikation verarbeitet werden. In manchen Fällen kann über Schwachstellen der Applikationen auch die Kontrolle über das zugrunde liegende System erlangt werden. Andere Applikationen des Angreifers (Schadsoftware) können auf diese Weise vom Nutzer unbemerkt installiert werden, um darüber wiederum Daten des Systems abzufangen oder auf das System selbst zuzugreifen.

  Es gibt auch Berichte über eingebaute Backdoors in kommerziellen Kryptoalgorithmen. Hierbei werden die Verschlüsselungsverfahren bewusst weniger gut umgesetzt. Häufig ist es ausreichend den Zufallszahlengenerator deterministischer zu machen als er eigentlich ist. Wenn die Anzahl der generierten Zufallszahlen überschaubar und dem Angreifer bekannt ist, dann sind Angriffe wesentlich schneller erfolgreich.

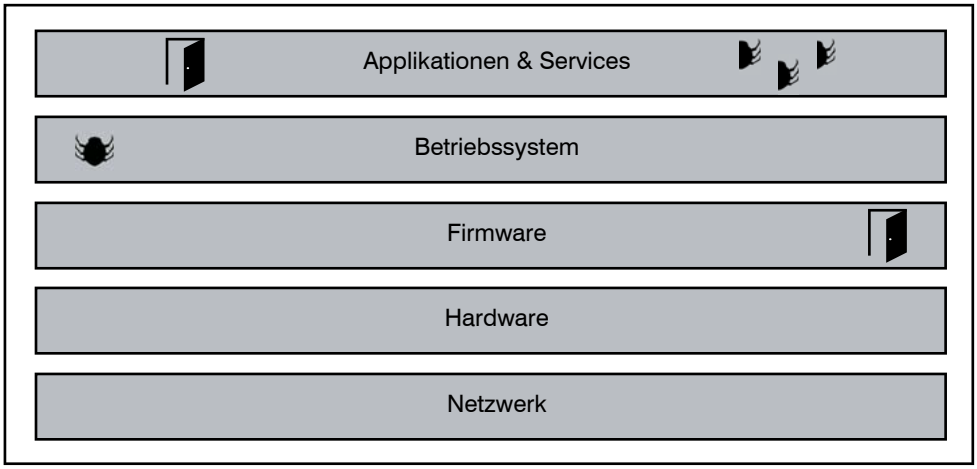


Abbildung 1: Ebenen eines IT-Systems aus der Angreiferperspektive

- **Betriebssystemebene**
  Eingriffe auf Betriebssystemebene erreichen nicht nur eine Anwendung oder einen Hersteller, sondern ermöglichen häufig den Zugriff auf alle Anwendungen und Daten, die auf diesem Betriebssystem (auf einem Client) installiert sind.

  Zu den wichtigsten Betriebssystemen aus der Perspektive eines Geheimdienstes (oder eines ähnlich versierten Angreifers) mit der Absicht, einen Verdächtigen zu beobachten, gehören bei den Desktopsystemen heutzutage Windows und OS X. Bei den mobilen Endgeräten sind insbesondere die Betriebssysteme Android, iOS und Windows Phone weit verbreitet. Alle Hersteller dieser Betriebssysteme (Apple, Microsoft und Google) sind den Dokumenten von Edward Snowden zufolge durch Gesetze wie FISA zur Kooperation mit den vereinigten Staaten verpflichtet.

  So ist es theoretisch möglich, dass Smartphones mit den oben erwähnten Betriebssystemen Backdoors haben oder Exploits (programmtechnische Möglichkeiten zur Manipulation von PC-Aktivitäten) erlauben, die auf Betriebssystemebene Zugriff auf die Inhalte und Kommunikation des Smartphone-Nutzers ermöglichen. Jedoch können auch Sicherheitslücken, welche unabsichtlich in einem Betriebssystem enthalten sind, Möglichkeiten für einen solchen Angriff bieten.

  Aus diesem Grund ist die Anzahl von Sicherheits-Features bei Smartphones in den vergangenen Jahren rapide gestiegen. So gehören beispielsweise Verschlüsselungen des internen und externen Speichers mittlerweile zur Standardausstattung eines Smartphones. Das iPhone 6 verschlüsselt beispielsweise seinen internen Speicher mit AES

# Der Netzwerk Insider

## Systematische Weiterbildung für Netzwerk- und IT-Professionals

256 Bit. Zudem wird der Schlüssel zum Entschlüsseln des Speichers bei jedem Herunterfahren des Gerätes gelöscht. Der Schlüssel kann nur durch die Eingabe der PIN wiederhergestellt werden. Zusätzlich kann der Benutzer ein Feature aktivieren, mit welchem bei 10-facher Falscheingabe der PIN der gesamte interne Speicher des iPhones gelöscht wird. Ähnliche Mechanismen kommen auch bei anderen Smartphones zum Einsatz oder sind zumindest für die Zukunft geplant.

Diese Art der Verschlüsselung, welche vom Endbenutzer immer häufiger als Schutz vor unberechtigtem Zugriff genutzt wird, wurde in letzter Zeit schon häufiger kritisiert. So seien beispielsweise in Fällen von Kidnapping direkte Maßnahmen, welche die Entschlüsselung eines gefundenen iPhones als Grundlage haben, nicht mehr möglich. NSA-Chef Michael Rogers hat daher laut einem Bericht der Washington Post angeregt, dass Hersteller Zugriffscodes für verschlüsselte Smartphones und Computer erstellen sollen, welche den Zugriff auf diese Geräte ermöglichen. Die Zugangscodes sollen dann in einzelnen Teilen bei unterschiedlichen Institutionen hinterlegt werden. Bei Bedarf können sich die Institutionen dann ihre Schlüssel kombinieren und auf das entsprechende Gerät zugreifen.

- **Firmware**
  Ein Eingriff auf Firmware- / Treiber-Ebene ermöglicht das Abgreifen von Informationen unabhängig vom Betriebssystem. Solche Eingriffe können sowohl über ungewollt auftretende Sicherheitslücken, als auch über bewusst eingebaute Backdoors erfolgen. So können beispielsweise Backdoors im BIOS angelegt werden, die nach einem PC-Start auf Betriebssystem- und Applikationsebene ausgenutzt werden können.

  Den Dokumenten von Edward Snowden zufolge war eine solche Backdoor im BIOS verschiedener Systeme (u.a. von Dell PowerEdge Servern) der NSA zuzuordnen. Software, um diese Backdoor im BIOS zu implementieren, wird im NSA ANT Katalog unter der Bezeichnung DEITYBOUNCE aufgeführt. Der NSA ANT (Advanced Network Technology) Katalog ist ein angebliches Dokument der NSA, welches sowohl Hardware als auch Software auflistet, mit der Spionage auf IT-Ebene betrieben werden kann. Die dort gelisteten Elemente können von der NSA selbst als auch von ausgewählten verbündeten Staaten erworben werden.

  Zu solcher Hardware gehören auch kleine Hardwarekomponenten, welche beispielsweise in Routern von Nerzwerkausrüstern implementiert werden. Laut den Snowden-Dokumenten werden hierzu Bestellungen von großen Netzwerkausrüstern gezielt abgefangen, mit entsprechenden Hardwarekomponenten ausgestattet (verwanzt) und anschließend wieder versiegelt und weiterversandt. Ein solches Vorgehen spielt sich vermutlich ohne das Wissen der Hersteller ab und scheint nicht durch Gesetze wie FISA abgedeckt zu sein.

- **Netzwerkebene**
  Daten, welche über ein Netz übertragen werden, können von einem Angreifer abgegriffen werden. Ein Angreifer kann alle Daten, welche über eine bestimmte Verbindung gesendet werden, abfangen und auf einem eigenen System speichern.

  Auf Grund der hohen Datenmenge, die heutzutage über das Internet versandt wird, ist es in der Regeln nicht praktikabel alle Informationen abzufangen und zu speichern. Bei einem Angriff auf Netzwerkebene können daher zwei Strategien verfolgt werden. Es können blind Nachrichten abgefangen und ausgewertet werden. Die Speicherung interessanter Daten erfolgt dann nach Auswertung der Daten. Diese Art des Abfangens von Informationen ist allerdings sehr mühsam und es ist nicht garantiert, dass die Informationen, welche man auf diesem Weg erhält für den Angreifer sinnvoll sind.

  Alternativ können gezielt Nachrichten abgefangen werden, welche von einem bestimmten Router aus oder an einen bestimmten Server gesandt werden, indem der Angreifer gezielt diese Verbindung abhört. Auf diese Art sind Angriffe auf bestimmte Personen (falls bekannt ist, von wo aus diese kommunizieren) oder auf bestimmte Dienste (abhören der entsprechenden Server) möglich.

  Staaten und Hackergruppen können bei Angriffen auf Kommunikationswege wesentlich mehr Daten von unterschiedlichen Quellen abfließen lassen. Diese werden zunächst in Data Centern gespeichert und bei Bedarf mit Big Data-Ansätzen analysiert. Bei solchen Angriffen sind die angreifenden Gruppen beispielsweise an den Meta-Informationen interessiert. Hieraus lässt sich ohne große Aufwände rekonstruieren, wer mit wem zu welcher Zeit kommuniziert. Allerdings ist das Abfangen von Daten auf Netzwerkebene mit sehr hohem Auf-

# Der Netzwerk Insider

Systematische Weiterbildung für Netzwerk- und IT-Professionals

wand verbunden, da die abgefangenen Daten insbesondere gezielt nach den gewünschten Informationen durchsucht werden müssen.

### 1.3 Schutzmaßnahmen

Um die eigenen Daten bei der Aufbewahrung, Verarbeitung und Kommunikation zu schützen, kann man unterschiedliche Maßnahmen umsetzen. Einige dieser Maßnahmen und die Grundlagen zu diesen stellen wir im Folgenden vor.

#### 1.3.1 Grundlagen zur Verschlüsselung und Tor-Verbindungen

- **Verschlüsselung**
  Eine einfache Möglichkeit zur Verschlüsselung bieten symmetrische Verschlüsselungsalgorithmen. Bei der symmetrischen Verschlüsselung wird der gleiche Schlüssel zur Ver- und Entschlüsselung genutzt. Das bedeutet, dass der Schlüssel, wenn er zweimal auf den gleichen Text angewandt wird, wieder den ursprünglichen Text ergibt. Das hat jedoch den Nachteil, dass der Schlüssel auf sicherem Weg ausgetauscht werden muss, da jeder, der Kenntnis über den Schlüssels erlangt, in der Lage ist, den Text wieder zu entschlüsseln.

  In der Praxis werden häufig Verschlüsselungsalgorithmen genutzt, welche ein Public-Key-Verfahren zur Ver- und Entschlüsselung nutzen. Bei der Public-Key-Verschlüsselung (asymmetrische Verschlüsselung) hat jeder Teilnehmer einen öffentlichen Schlüssel, welchen er nach außen hin bekannt gibt, und einen privaten Schlüssel, welcher nur dem Teilnehmer selbst bekannt ist.

  Zwischen dem öffentlichen und dem privaten Schlüssel besteht ein mathematischer Zusammenhang. Jedoch kann man, wenn man einen der beiden Schlüssel kennt, den anderen ohne Kenntnis der dahinter liegenden Formel nicht berechnen. Der öffentliche Schlüssel kann zur Verschlüsselung einer Nachricht an den Teilnehmer verwendet werden. Die Entschlüsselung ist dann nur mit dem privaten Schlüssel des Teilnehmers möglich.

  Zur schnelleren Berechnung wird normalerweise nicht die ganze Kommunikation mittels asymmetrischer Verschlüsselung verschlüsselt, da die Berechnung dieser sehr langsam ist. Asymmetrische Verschlüsselung wird lediglich genutzt, um einen zufällig erzeugten symmetrischen Schlüssel zu verschlüsseln. (siehe Abbildung 2)

  Voraussetzung, um die Sicherheit einer mittels asymmetrischer Verschlüsselung verschlüsselter Nachricht zu garantieren, ist allerdings, dass die Schlüssel sicher verwaltet werden.

- **Tor**
  Bei Tor handelt es sich um einen Anonymisierungsdienst, welcher Datenströme verschleiert. Bei der Nutzung von Tor wird der Datenverkehr nicht direkt vom Start zum Ziel geroutet, sondern die Route wird über zufällige Zwischenziele geroutet.

  Der Client muss dabei eine entsprechende Software installieren. Über diese Software werden verfügbare Tor-Knoten ermittelt. Sie verbindet sich dann mit einem Tor-Knoten und handelt mit diesem eine verschlüsselte Verbindung aus. Dieser Tor-Knoten wiederum handelt dann mit dem nächsten Tor-Knoten eine verschlüsselte Verbindung aus. Dies wird fortgesetzt, bis drei Zwischenserver gewählt wurden, um eine möglichst gute Anonymität zu erreichen, dabei die Übertragung aber nicht unnötig zu verzögern.

  Die Übertragung vom Client zum ersten Tor-Knoten und zwischen den Tor-Knoten erfolgt dabei verschlüsselt. Nur die Verbindung zwischen dem letzten Tor-Knoten und dem Ziel erfolgt unverschlüsselt. Es ist einem Angreifer so möglich, die Kommunikation zwischen dem letzten Tor-Knoten und dem Ziel-Server abzuhören. Allerdings ist das Netzwerk so aufgebaut, dass es einem Angreifer nicht möglich ist, die Kommunikation zum Startpunkt zurück zu verfolgen. (siehe Abbildung 3)

#### 1.3.2 Maßnahmen in der Praxis

Möchte man sensible Informationen vor Angriffen schützen, so ist die sicherste Schutzmaßnahme nach wie vor ein klassischer „Air Gap“. Hierbei werden die sensiblen Informationen auf Systemen hinterlegt, welche keinen Zugriff auf das Internet haben und an kein Netzwerk angebunden sind (weder kabelgebunden noch kabellos). Komponenten zur Anbindung an ein Netzwerk sind dabei entweder gar nicht erst installiert oder deaktiviert. Der Austausch von Informationen mit diesen Systemen geschieht über externe Datenträger (z.B. USB-Sticks). Dabei werden die Daten häufig verschlüsselt zwischen den Systemen übertragen. Dies ist bis heute die einzige Maßnahme um einen Angriff auf die Daten fast vollständig auszuschließen.

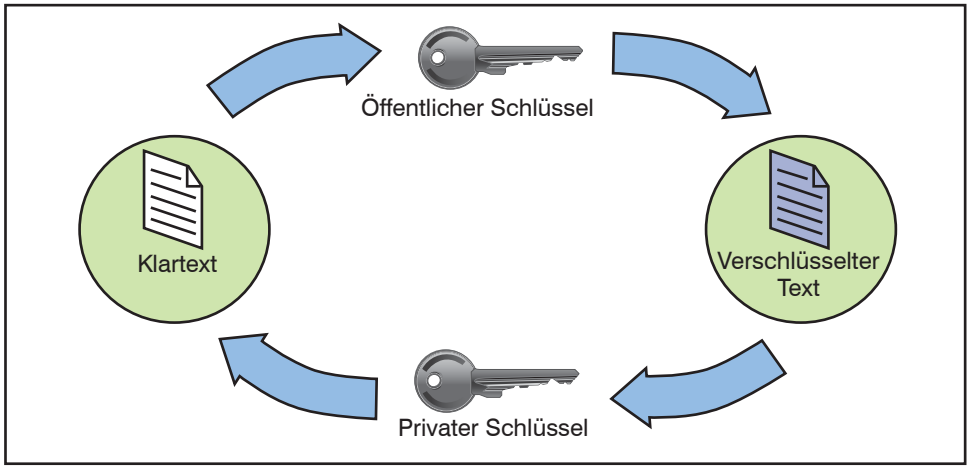


Abbildung 2: Asymmetrische Verschlüsselung

# Der Netzwerk Insider

**Systematische Weiterbildung für Netzwerk- und IT-Professionals**

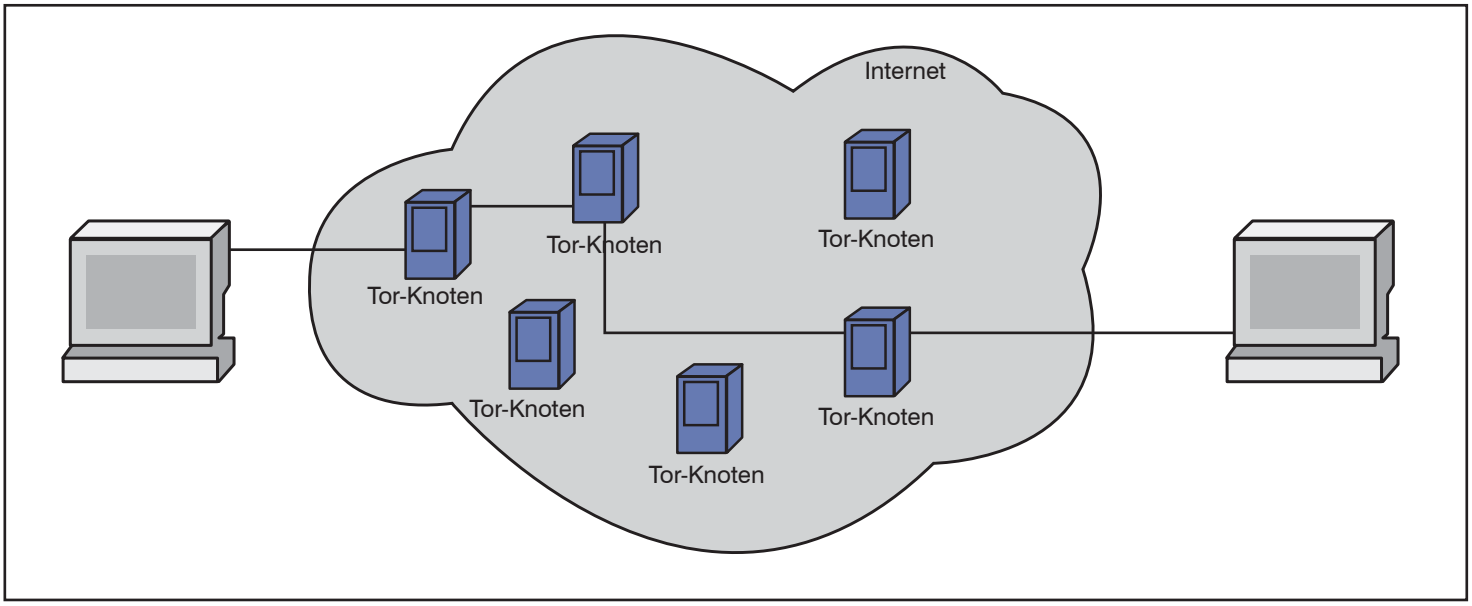


Abbildung 3: Zufällige Wahl einer Route über Tor-Knoten

In der Praxis ist ein solcher „Air Gap“ allerdings meist nicht praktikabel. Im Folgenden werden daher verschiedene Maßnahmen aufgelistet, welche zu einer erhöhten Sicherheit von Informationen beitragen können. Diese können zwar das Risiko eines Angriffs bzw. der Folgen durch einen Angriff verringern, sie bieten jedoch keinen absoluten Schutz vor Angriffen:

- **Verwendung von Anonymisierungsdiensten:** Durch die Verwendung von Anonymisierungsdiensten (wie Tor) wird der Kommunikationsdatenstrom verschleiert und bei jedem Verbindungsaufbau über ein anderes Gateway ins Internet geleitet. Somit kann der Angreifer den interessanten Datenstrom schwer identifizieren.

- **Verschlüsselung der Datenströme:** Die Datenströme sollten stets verschlüsselt sein (z.B. Verwendung von TLS und IPSec). Obwohl auch solche Datenströme gegebenenfalls entschlüsselt werden können, so ist der Aufwand doch wesentlich höher als unverschlüsselte Daten zu lesen. Je aufwendiger die Entschlüsselung von Daten ist, desto unwahrscheinlicher ist es, dass ein Angreifer diese einsehen möchte und kann. Dabei sollten so viele Datenströme verschlüsselt werden, wie möglich / sinnvoll. So gibt es beispielsweise HTTPS-Everywhere Browser Addons, welche bei Webseiten, die es sowohl verschlüsselt als auch unverschlüsselt gibt, stets den verschlüsselten Zugang wählen.

- **Nutzung von Browser in a Box:** Browser in a Box ist eine Lösung um geschützt im Internet zu Surfen und E-Mails zu empfangen. Bei Browser in a Box Lösungen wird ein Browser auf einem reduzierten Betriebssystem in einer virtuellen Maschine gekapselt. Malware, welche beim Surfen im Internet oder durch Öffnung des Anhangs einer E-Mail auf das Betriebssystem gelangt, kann sich durch die Kapselung nicht weiter auf das Hostsystem ausbreiten. Kommuniziert das Hostsystem ausschließlich über den Bowser in a Box mit dem Internet, ist vor Angriffen durch Schadsoftware weitgehend geschützt. Das Betriebssystem, auf welchem der Browser läuft, kann bei einer Infektion jederzeit auf einen definierten Ausgangszustand zurückgesetzt werden.

  Ein Beispiel für einen Browser in a Box ist BitBox, welches im Auftrag des BSI entwickelt worden ist. Hinsichtlich der Praktikabilität solcher Ansätze ist jedoch anzumerken, dass für viele Anwendungsfälle die Box für einen Datenaustausch kontrolliert geöffnet werden müsste (z.B. zur Datenübertragung an das Hostsystem), was die Sicherheit oder die Nutzbarkeit deutlich reduzieren kann oder bei entsprechend starker Reglementierung der Öffnung der Box die Nutzbarkeit der Lösung einschränkt.

- **Kritische Analyse bei der Softwarebeschaffung:** Viele Berichte deuten darauf hin, dass große Softwareunternehmen für die Regierungen der Länder, in denen sie wirtschaften, Backdoors einbauen müssen. Dies trifft sowohl für Unternehmen zu, die Betriebssysteme verkaufen als auch für solche, die Antivirenprogramme, Verschlüsselungs- und Router-Software bereitstellen. Diese Backdoors können auch von anderen Angriffsgruppen als der landeseigenen Regierung ausgenutzt werden. Wenn eine solche Backdoor bekannt wird, vertuschen viele Unternehmen dies häufig als Versehen und veröffentlichen einen entsprechenden Patch.

  Häufig kann es daher sinnvoll sein auch

# Der Netzwerk Insider

## Systematische Weiterbildung für Netzwerk- und IT-Professionals

die Nutzung von Open Source Software zu prüfen. Da diese öffentlich entwickelt und geprüft werden kann, ist es bei dieser Art von Software deutlich unwahrscheinlicher, dass in diese Software Backdoors eingebaut worden sind.

- **Ende-zu-Ende Verschlüsselung verwenden:** Bei Kommunikation über öffentliche Netzwerke sollte stets Ende-zu-Ende Verschlüsselung verwendet werden. Es ist generell darauf zu achten, dass der private Schlüssel nur dem Eigentümer bekannt ist. Bei Ende-zu-Ende Verschlüsselung werden die Daten vom Sender der Daten verschlüsselt. Die kodierten Daten werden anschließend übertragen und können nur vom Empfänger wieder entschlüsselt werden. Es erfolgt keine Entschlüsselung der Daten auf dem Transportweg.
  Ein Beispiel für eine Ende-zu-Ende Verschlüsselung mittels Public-Key-Verfahren ist die Verschlüsselung von E-Mails mittels PGP (Pretty Good Privacy) oder S/MIME (Secure / Multipurpose Internet Mail Extensions). S/MIME wird mittlerweile von den meisten E-Mailprogrammen nativ unterstützt. Für die Verwendung von PGP ist hingegen meist die Installation eines Plug-Ins erforderlich. Kürzlich wurde bekannt gegeben, dass De-Mail PGP nun über ein Browser-Plugin nativ unterstützt.

  Da E-Mails bei der Ende-zu-Ende Verschlüsselung jedoch verschlüsselt versandt und gespeichert werden, ist es nicht mehr möglich, diese einfach auf dem Webserver zu lesen oder von einem beliebigen Endgerät abzurufen. Dies ist nur noch von Endgeräten aus möglich, welche diese Verfahren unterstützen und welchen, der der persönliche Schlüssel des Empfängers bekannt ist. Aus diesem Grund werden in der Praxis viele Mails immer noch unverschlüsselt versandt.

  Eine weitere Anwendung für die Ende-zu-Ende Verschlüsselung ist die Verschlüsselung von Telefonaten oder Textnachrichten mittels Verschlüsselungsapplikationen. Dies setzt allerdings voraus, dass beide Gesprächspartner die gleiche Applikation installiert haben. Beispiele für Applikationen zur Verschlüsselung von Telefonaten sind Red Phone (Android), Signal (iPhone) oder Cellcrypt (für unterschiedliche Betriebssysteme). Textnachrichten können über Applikationen wie Cryptochat und Red Phone ausgetauscht werden.

- **Datenspeicher verschlüsseln:** Bei einem unbefugten Zugriff auf ein System(PC, Server, Datenbanken, etc.) ist es wesentlich schwieriger Informationen zu extrahieren, wenn die dort hinterlegten Daten verschlüsselt sind. Viele Betriebssysteme, auch von mobilen Endgeräten (iOS, Android, Windows Phone, …), bieten bordeigene Mittel zur Verschlüsselung des Speichers an.

- **Angemessene Passwortrichtlinien bzw. Wahl eines angemessenen Passworts:** Um die Sicherheit eines Passwortes zu gewährleisten, sollte dieses ausreichend komplex und lang sein. Hierzu gibt es zahlreiche Richtlinien im Internet, aktuelle Empfehlungen dazu können beispielsweise auf den Internetseiten des BSI gefunden werden. Wenn das Passwort anderweitig beschafft werden kann, dann bringt diese Maßnahme keinen Schutz. Daher ist zusätzlich - soweit möglich - sicherzustellen, dass Unbefugte keinen Zugriff auf das Passwort erhalten. Die angemessene Wahl eines Passworts ist vor allem bei Dictionary und Brute Force Angriffen essentiell.

- **Zwei-Faktor-Authentisierung:** Für den Zugang zu besonders sensiblen Bereichen sollte ausschließlich eine Zwei-Faktor-Authentisierung genutzt werden. Diese besteht aus einer fixen Anmeldeinformation (z.B. ein selbst gewähltes Passwort) und einer variablen Anmeldeinformation (z.B. ein temporärer Code den man zu jeder Anmeldung auf sein Smartphone erhält).

  Bei vielen Diensten ist es mittlerweile möglich eine Zwei-Faktor-Authentisierung zu wählen. Diese ist jedoch normalerweise nicht standardmäßig aktiviert, sondern sie muss vom Nutzer bewusst ausgewählt werden.

- **Antivirenprogramme regelmäßig aktualisieren:** Die Installation eines Antivirenprogramms, sowie einer Firewall sollten heutzutage für jeden selbstverständlich sein. Jedoch wird stets neue Schadsoftware entwickelt, welche Angreifern die Möglichkeit bietet unbefugt auf Daten eines Systems zuzugreifen. Daher ist es notwendig, auch die Programme, die diese Schadsoftware finden und entfernen sollen, regelmäßig zu aktualisieren. Nur so ist sichergestellt, dass die Antivirensoftware aktuelle Schadsoftware auch erkennt und diese vom System entfernen kann. Nur so ist gewährleistet, dass die Angriffsfläche eines Systems möglichst gering gehalten wird.

- **Aktuelle Sicherheits-Patches installieren:** Betriebssysteme und andere Soft-

# Der Netzwerk Insider

## Systematische Weiterbildung für Netzwerk- und IT-Professionals

ware weisen häufig Sicherheitslücken auf, welche zum Zeitpunkt der Installation noch nicht bekannt waren. Über diese Sicherheitslücken ist es möglich ein System anzugreifen und Daten des betroffenen Systems abzufangen. Angriffe über öffentlich bekannt gewordene Sicherheitslücken, für welche aber bereits Patches existieren, treten vermehrt auf. Sicherheits-Patches, welche diese Sicherheitslücken schließen, sind daher umso notwendiger, um das Angriffsrisiko zu minimieren.

- **Standardisierte Produkte verwenden:** Cyberangreifer können, indem sie sich Zugriff auf den Quellcode verschaffen, Backdoors in Software einbauen. Da der Quellcode proprietärer Software (z.B. Bitlocker) nicht öffentlich zugänglich ist, fallen Backdoors in proprietärer Software deutlich seltener auf, als in öffentlicher (bspw. TLS-Implementierungen). Daher sind Implementierungen allgemeingültiger Standards (RFCs, IEEE Standards, etc.) häufig sicherer gegen Angreifer als proprietäre Software.

- **Übergreifende Analyse und Kontrolle zur Bekämpfung von Angriffen:** Durch den Einsatz einer Plattform-, System- und anwendungsübergreifenden Analyse und Kontrolle sollen auch neuartige Cyberangriffe wie APT-Angriffe oder Zero-Day-Exploits erkannt und gezielt bekämpft werden. Hierfür kommen in Ergänzung zu herkömmlichen Sicherheitssystemen, wie Firewalls, Intrusion Prevention Systemen (d.h. Systemen zur Abwehr von Angriffen, kurz: IPS), Data Loss Prevention (d.h. Systemen, zum Schutz vor unerwünschtem Datenabfluss, kurz: DLP) und Antivirenprogrammen, Sicherheits-Intelligenzen zum Einsatz.

  Traditionell wird dieses Themengebiet durch sogenannte Security Information und Event Management (SIEM) Systeme bedient, welche eine Analyse von Sicherheitsmeldungen verschiedener Komponenten in Echtzeit auswerten. Deren weitere Entwicklungsstufe ist nun Bedrohungs- und angriffsfokussiert. Solche 2nd Generation SIEM, oder auch Next-Generation-Threat-Protection (NGTP) Systeme wenden verschiedene (auch signaturunabhängige) Analysen an, um zielgerichtete und mehrstufige Angriffe zu erkennen. NGTP verfolgen das Ziel auch Schadsoftware und Angriffe zu erkennen, welche bisher unbekannt sind und durch herkömmliche Sicherheitssysteme daher noch nicht erkannt werden können.

  Um die notwendigen Informationen für solche Intelligenzen zu sammeln, werden Endgeräte (Clients, Server) aber auch Netzwerkkomponenten (insbesondere solchen mit Firewall-Funktion) mit einer Sensorik im Sinne von Intrusion Detection Systemen (IDS) ausgestattet. So kann ggf. der Angriff schon dort festgestellt werden, wo er geschieht. Außerdem werden die so erweiterten Komponenten befähigt ein kontextuelles Bewusstsein für die Nutzer, Anwendungen, Kommunikation u.Ä. zu entwickeln. Ein Bespiel für eine solche Sensorik sind die FirePOWER Produkte von Cisco und ein Beispiel für eine NGTP-Lösung ist die Threat Analytics Platform von FireEye.

- **Nutzung von Big Data zur Angriffserkennung:** Big Data bedeutet hier die Sammlung und Auswertung großer Datenmengen mit Relevanz in der Informationssicherheit, wie beispielsweise über traditionelle SIEM ausgewertete Daten, aber auch Netzwerkverkehr, Nutzeraktivitäten uvm. Big Data wird in der Informationssicherheit zur Analyse von Merkmalen bei zielgerichteten Angriffen genutzt. Big Data Tools helfen die vorhandenen Daten effektiv auszuwerten und ermitteln Muster bzw. anderen Indizien zur Identifizierung potentieller Angriffe. Auf diese Weise können Sicherheits-Intelligenzen wie NGTP auf ein mächtiges Analysewerkzeug zurückgreifen und aus der Masse der zur Verfügung stehenden Informationen potentielle Angriffe herausfiltern. Ein Beispiel für die Anwendung von Big Data in der Informationssicherheit ist die Nutzung von Daten aus IBM InfoSphere BigInsights im IBM Security QRadar.

- **Interagierende Plattformen:** Heutige Cyberangriffe zielen in der Regel nicht nur auf eine Komponente ab, sondern erstrecken sich über verschiedene Plattformen, Ebenen und Komponenten des angegriffenen Systems. Daher sind interagierende Plattformen, welche bei einem Angriff zur Erhöhung des Schutzes Informationen austauschen und sich organisieren, eine gute Methode Angriffen entgegenzutreten.
  Hierbei bekommen diverse Netzwerkkomponenten neben einer Sensorik, um z.B. aus dem Datenverkehr die Art, den Nutzer, oder die Anwendung zu erkennen und zu melden, zusätzlich die Fähigkeit auf Ereignisse zu reagieren. Falls beispielsweise eine Sicherheits-Intelligenz eine verdächtige Verhaltensanomalie in der Infrastruktur feststellt, kann sie über einen Alarm hinaus aktiv werden. Sie kann beispielsweise die Firewall kontaktieren, damit diese den Verkehr von und zur Quelle des Angriffs blockiert.

  Zudem könnte über die Sicherheits-Intelligenz die NAC-Lösung (z.B. RADIUS Server) informiert werden, damit diese das Endgerät, von dem ein Angriff ausgeht (z.B. ein Endgerät, dass mit einem RAT infiziert ist), vom normalen Netz abkoppelt und in Quarantäne ausgliedert. Damit wird verhindert, dass sich ein Angriff über das betroffene System hinaus ausbreitet. Ein Beispiel für ein Produkt, was eine solche Sicherheits-Intelligenz implementiert, ist Damballa Filesafe.

- **Nutzung von Endpoint Visibility, Access, and Security (EVAS) zur Netzzugangskontrolle:** NAC-Lösungen steuern den Zugriff von Endgeräten auf ein Netzwerk. Bei traditionellen NAC-Lösungen erfolgt der Zugang von Endgeräten zum Netz gemäß der Konfiguration des gewählten Zugangspunkts, wobei der gewünschte Zugriff jedoch nur nach erfolgreicher Authentisierung erfolgen darf. Mit EVAS wird die Steuerung des Zugangs zu einem Netz erweitert. Dies geschieht mithilfe einer detaillierten, kontextuellen Prüfung gemäß betrieblicher Anforderungen, wie beispielsweise der Rolle des Anwenders, des Orts und der Zeit des Zugriffs, Forderungen der Geschäftsprozesse etc. Über eine Überwachung der übertragenen Daten und einer Anbindung an bestehende Systeme wie SIEM, Next-Generation-Threat-Protection oder andere Präventionssysteme können außerdem Angriffe auf das Netzwerk frühzeitig erkannt und unterbunden werden.

# Der Netzwerk Insider

Systematische Weiterbildung für Netzwerk- und IT-Professionals

### 1.4 Grenzen des Schutzes

Es gibt Möglichkeiten die hier vorgestellten Schutzmaßnahmen zu umgehen. So kann die Verschlüsselung von Nachrichten als Unbefugter beispielsweise umgangen werden, um Nachrichten trotz Verschlüsselung zu lesen. Eine dieser Möglichkeiten ist es die Nachricht auf dem System, von welchem sie gesendet wird, vor der Verschlüsselung abzufangen und an eine eigene E-Mail-Adresse oder einen eigenen Server weiterzuleiten. Dies ist beispielsweise über das Einschleusen von eigener Schadsoftware (z.B. über RAT wie „EquationDrug“) auf Rechnern von Personen, deren Nachrichten gelesen werden sollen, möglich.

Auch gibt es bisher keinen wirksamen Schutz gegen Angriffe, welche über Backdoors in Software erfolgen, bei denen der Hersteller die Daten an Dritte freigibt. Zwar kann in manchen Fällen das Risiko einer Backdoor durch geschickte Auswahl der eigenen Software minimiert werden, jedoch ist es nicht möglich, solche Angriffe vollständig zu vermeiden.

Um solche Angriffe in Zukunft besser erkennen zu können, werden übergreifende Analysen und interagierende Plattformen benötigt. Um konsistente und mächtige Schutzmaßnahmen im Rahmen von interagierenden Plattformen und Netzwerken mit Sicherheits-Intelligenz in heterogenen Umgebungen jedoch möglich zu machen, werden diesbezüglich neue und übergreifende Standards benötigt. Diese Standards müssen von den beteiligten Plattform-Herstellern dafür genutzt werden, die Inter-Plattform Kommunikation zu erlauben. So können unterschiedliche kommerzielle Lösungen von konkurrierenden Unternehmen in einem Kunden-Setup eine lückenlose und einheitliche Sicherheitskonzeption auf Ebene der interagierenden Plattformen ermöglichen. Eine Standardisierung dieser Art fehlt jedoch heute noch häufig.

Dieses Thema könnte bauartbedingt durch Software-Defined Networks (SDN) bedient werden. Sensoren für Bedrohungserkennungen im Sinne von IDS Systemen könnten über bereits vernetzte und interagierende Systeme in SDNs eine Bedrohung frühzeitig erkennen und mehrstufige Angriffe bekämpfen. Die SDN-Gemeinde greift das Thema der Informationssicherheit aber erst seit kurzem ernsthaft auf und dies spiegelt sich daher bislang auch kaum in Produkten wieder. Neue Entwicklungen in diesem Bereich sind daher mit Spannung abzuwarten.

### 1.5 Fazit

Eine Kombination der hier vorgestellten Maßnahmen kann nicht gänzlich verhindern, dass Daten abgegriffen werden können. Jedoch werden die Hürden und das Risiko für einen Zugriff durch Angreifer deutlich höher gesetzt. Ein Angriff auf ein gut gesichertes System kostet viel Zeit und Aufwand. Nur so wird auch die Möglichkeit gegeben einen Angriff zu erkennen, nachzuverfolgen und schnell darauf zu reagieren.

Da sich die Angriffsmethoden immer wieder verändern und vielschichtiger werden, müssen das auch die Abwehrmechanismen. Traditionelle und seit langem genutzte Sicherheitsmechanismen stellen heutzutage eine wichtige Basis dar und haben trotz immer neuer Angriffsformen auch weiterhin ihre Berechtigung. Sie müssen jedoch durch auf neue Angriffsformen angepasste Maßnahmen ergänzt werden, um weiterhin einen hohen Schutz gegen Angriffe sicherzustellen. So gehören Maßnahmen zur übergreifenden Kontrolle und Überwachung beispielsweise zu den unbedingt notwendigen Best Practices, wenn stark vernetzten Angreifern mit ihren weitreichenden Überwachungsmöglichkeiten ein Netzwerk an Angriffserkennung entgegengesetzt werden soll. Bei schützenswerten Daten sollten diese daher konsequent und unternehmensweit eingesetzt werden.