Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260
Herausgegeben von Stefan Schumacher
Erschienen im Magdeburger Institut für Sicherheitsforschung
http://www.sicherheitsforschung-magdeburg.de/publikationen/journal.html

Informationssicherheit in Versorgungsunternehmen umsetzen

Einige praktische Erfahrungen

Stefan Schumacher

Versorgungsunternehmen sind als Betreiber kritischer Infrastrukturen vielfältigen Angriffen aus dem Internet ausgesetzt. Sowohl einfache Bürorechner, Abrechnungssystem als auch Industriesteuerungsanlagen werden regelmäßig von verschiedenen Akteuren attackiert. Darunter fallen auch ungezielte automatisierte Massenangriffe.

Der Beitrag zeigt, wie Sie Ihre Infrastruktur vor Angriffen schützen können, wie Sie dazu strategisch vorgehen müssen und welche technisch-organisatorische Maßnahmen implementiert werden sollten. Desweiteren werden in einem Überblick Standards bzw. Richtlinien wie ISO 27001 oder das BSI Grundschutzkonzept vorgestellt.

Dies ist eine überarbeitete Fassung des Beitrages zum Thüringer Wasserkolloquium 2017, erschienen als Schumacher, S. (2017). Informationssicherheit in Versorgungsunternehmen umsetzen, In *22. Thüringer Wasserkolloquium*, Erfurt, Fachhochschule Erfurt

Keywords: Informationssicherheit, Versorgungsunternehmen, Trinkwassertagung

Zitation: Schumacher, S. (2020). Informationssicherheit in Versorgungsunternehmen umsetzen: Einige praktische Erfahrungen. *Magdeburger Journal zur Sicherheitsforschung*, *20*, 995–1002. Verfügbar 29. Dezember 2020 unter http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS_070_Schumacher_Versorgungsunternehmen.pdf

1 Einführung

Gerade viele kleinere Unternehmen, Behörden und Versorger sind der Meinung, dass sie nicht das Ziel von Angriffen werden. Oftmals begründen Sie dies damit, dass sie als Unternehmen zu klein und unbedeutend seien, um für Angreifer interessante Daten vorzuhalten.

Allerdings sind die meisten Angriffe, die über das Internet stattfinden nicht gezielte Angriffe gegen sorgfältig ausgewählte Ziele. Vielmehr nutzen einige Angreifer automatisierte Programme, um das Internet nach verwundbaren Rechnern abzusuchen und in diese ebenfalls vollautomatisiert einzubrechen.

So gibt es beispielsweise in Staaten der ehemaligen Sowjetunion Banden in der organisierten Kriminalität, die von ehemaligen Geheimdienstmitarbeitern geführt werden. Diese Banden verfügen daher nicht nur über exzellente Kenntnisse in der konspirativen Arbeit, sondern haben sich schon seit Jahren auf Cyberkriminalität spezialisiert. So werden regelmäßig gut ausgebildete Informatiker der russischen Universitäten von diesen Banden angestellt, um Wirtschaftsspionage oder Online-Erpressungen durchzuführen.

Eine einfache Methode ist der sogenannte Denial-of-Service-Angriff. Hierbei wird ein Server mit Anfragen derart überlastet, dass berechtigte Benutzer die Dienste nicht mehr in Anspruch nehmen können. Der Angreifer kann dazu zum Beispiel mehrere Rechner unter seine Kontrolle bringen und einen Webserver mit Anfragen soweit lahmlegen, das potenzielle Kunden den Webshop des Opfers nicht mehr aufrufen können. Damit wird entweder das Opfer direkt geschädigt oder es wird Schutzgeld erpresst. Zahlt das Opfer nicht eine gewisse Summe an die Erpresser, legen diese die Infrastruktur des Opfers lahm und fügen ihm so schweren wirtschaftlichen Schaden zu. Selbst wenn das Schutzgeld nur 500 Euro beträgt ergibt sich in der Summe ein einträgliches Geschäft bei relativ geringem Aufwand.

Problematisch ist hierbei in den letzen Jahren die leichte Verfügbarkeit von automatisierten Angriffs-Programmen. Während man vor einigen Jahren als Angreifer noch erheblich Zeit in die eigene Ausbildung investieren und dabei komplexe Probleme lösen musste, gibt es inzwischen Programme die Angriffe automatisieren und leicht zu bedienen sind. Damit sinkt die technische Hürde um einen Angriff erfolgreich durchzuführen massiv ab. Damit sind nicht mehr nur Hacker mit hoher Technikkompetenz in der Lage Angriffe durchzuführen sondern jeder der in der Lage ist ein Programm aus dem Internet herunterzuladen und ein paar Einstellungen vorzunehmen.

So wurden im Februar 2000 mehrere amerikanische Webseiten mit einer DoS-Attacke überlastet und lahmgelegt. Zu den Opfern zählten unter anderem Yahoo!, Fifa.com, Amazon.com, Dell, Inc., E*TRADE, eBay, und CNN, amerikanische Analysten schätzten den entstandenen Schaden auf mehr als eine Milliarde Dollar. Bei dem später identifizierten Angreifer handelte es sich um einen 15-jährigen kanadischen Schüler. Er hatte im Internet ein Angriffswerkzeug gefunden und aus Langeweile mehrere bekannte Webseiten eingegeben und damit lahmgelegt.

Inzwischen sind die Angriffswerkzeuge wesentlich einfacher und raffinierter geworden. So gibt es Programme, die vollautomatisiert Rechner im Internet scannen. Der Angreifer kann dazu ein beliebiges Netzwerk (z.B. ein Unternehmen, eine Universität oder einen Internetanbieter in einem bestimmten Land) auswählen. Das Programm scannt dann nach und nach alle Rechner die derzeit mit dem Internet verbunden sind und versucht das Betriebssystem und darauf laufende Anwendungen bzw. Dienste zu erkennen. Dann vergleicht es die gefundenen Versionen mit einer Schwachstellendatenbank. Findet es eine Schwachstelle im System, kann es diese automatisch ausnutzen und den Rechner unter die Kontrolle des Angreifers bringen. Danach installiert es einen versteckten Zugang für den Angreifer und wartet auf weitere Befehle. Viele Angreifer nutzen derartige Werkzeuge um sich sogenannte Botnetze aufzubauen, die sie für weitere kriminelle Machenschaften verwenden. So werden viele Spam- und Betrugsmails über Botnetze versandt, ebenso werden unter anderem Raubkopien darüber verteilt oder Server mit verteilten DoS-Attacken lahmgelegt. Die technische Kompetenz, um sich ein solches Botnetz aufzubauen, ist inzwischen so niedrig, dass Sie sie sich innerhalb eines Tages aneignen können. So finden Sie allein auf Youtube tausende Tutorials in denen gezeigt wird wie sie die entsprechenden Angriffswerkzeuge finden, installieren und konfigurieren können.

Das größte bisher enttarnte Botnetz, BredoLab, hatte etwa 30.000.000 Rechner unter seiner Kontrolle, die Botnetze Mariposa und Conficker etwa 13.000.00 bzw 9.000.000 Rechner. Das Botnetz Rustock bestand aus etwas 1.700.000 Zombies und wurde genutzt, um täglich ca. 44 Milliarden Spammails zu verschicken. Mit dem Zugang zu den trojanisierten Rechnern wird schwunghafter Handel betrieben, das heißt, sie können in versteckten Diskussionsforen im digitalen Untergrund Botnetze kaufen oder mieten, um damit Konkurrenten anzugreifen. Ebenso werden im Untergrund Sicherheitslücken und Programm zu deren Ausnutzung gehandelt oder vermietet. Sollten Sie selbst technisch nicht in der Lage sein diese Programme auszunutzen, können Sie auch direkt kriminelle Banden mit den Angriffen beauftragen. Für wenige hundert Euro können Sie so beispielsweise das Adressverzeichnis und die Kundenkartei eines Konkurrenten beschaffen lassen. Eine sehr detaillierte Analyse des Carna-Botnets finden Sie in Shukla (2015).

Auch Schadsoftware hat sich in den letzten Jahren massiv weiterentwickelt. So gibt es zur Zeit eine Epidemie von sogenannter Ransomware, also Erpresserschädlingen. Diese dringen in Computer ein, trojanisieren das Betriebssystem und versuchen sich im lokalen Netzwerk in andere Rechner und Geräte (Netzwerkfestplatten etc.) einzuschleusen. Danach suchen sie auf den Festplatten nach bestimmten Dateien (Word, Excel, Po-

werpoint, OpenOffice.org, CAD, Bilder, Text etc.) und verschlüsseln diese Dateien. Das Opfer hat dann in der Regel 2-3 Tage Zeit, um auf ein verdecktes Konto 300-500 Euro Schutzgeld einzuzahlen. Angeblich erhält es nach erfolgter Einzahlung das Passwort zur Entschlüsselung der Dateien, eine Garantie dafür gibt es aber nicht. Das enttarnte CryptoDefense-Netzwerk verdiente mit dieser Masche ca. 38.000 US-Dollar im Monat (vgl. Chebbi, 2018; Fischer, 2018).

Häufig nutzen die Einbrecher bzw. die Scannerprogramme Datenbanken mit bekannten Sicherheitslücken um in Systeme einzubrechen. Daher ist es immens wichtig, verfügbare Updates für das Betriebssystem und Anwendungsprogramme (Flash, Java, Office etc.) unverzüglich einzuspielen. In dem Moment in dem Microsoft ein Update für eine Sicherheitslücke veröffentlicht kann auch der schlechteste Einbrecher ein Programm schreiben dass diese Sicherheitslücke ausnutzt. Es ist also ein Wettlauf mit der Zeit, ob Sie ihren PC aktuell und sicherer halten oder ob ein drittklassiger Einbrecher aus Rumänien Ihren PC unter seine Kontrolle bringt und darüber weitere Schadsoftware verteilt.

Neben ungezielten Massenangriffen gibt es auch noch elaborierte, gezielte Attacken. So hat z.B. die amerikanische NSA den Auftrag, Infrastrukturen weltweit zu penetrieren und unter ihre Kontrolle zu bringen. Daneben greifen auch Kriminelle Versorgungsunternehmen gezielt an, da diese bereit sind höhere Lösegeldsummen für ihre IT-Systeme zu zahlen (vgl. Schumacher, 2012a, 2012b, 2014a; Seidler, 2012; Weiße, 2012).

Selbst Angriffe mit Drohnen sind inzwischen Realität geworden (Brack, 2019), ebenso die inzwischen berüchtigten hochkomplexen Attacken gegen die ukrainische Stromversorgung mit der Schadsoftware BlackEnergy 3. Dabei wurden dem Versorger Прикарпаттяобленерго am 23.12.2015 30 Trafo-Stationen aus der Ferne abgeschaltet und 230 000 Ukrainer ohne Strom gelassen (Slowik, 2019).

Dabei werden inzwischen auch Angriffe auf die Supply-Chain immer elaborierter und häufiger. Holtmanns (2019), Kafka und Pfeiffer (2012) zeigt zum Beispiel Angriffe auf Mobile Core Networks, mit denen sich Mobilfunknetze groflächig lahmlegen oder manipulieren lassen. Dabei sind gerade Versorgungsunternehmen häufig auf die Verfügbarkeit dieser Technik angewiesen.

Um sich vor solchen gezielten Angriffen zu schützen, sind komplexere Maßnahmen notwendig. Dazu gehören vor allem eine adäquate Risikoanalyse und -bewertung, beispielsweise nach den BSI-Standards (Bundesamt für Sicherheit in der Informationstechnik, 2005a, 2005b, 2008a, 2008b, 2011). Alternativ können Sie auch auf die ISO2700x, ISO 19011 oder Cobit zurückgreifen (vgl. Feyrer, 2012, 2018).

2 Risikoanalyse und -bewertung

Der erste Schritt zur Überprüfung und Verbesserung der IT-Sicherheit ist die Risikoanalyse und -bewertung. Dazu werden die eingesetzte IT-Systeme (Hardware, Software und Prozesse) sowie ihre Sicherheitsfunktionen und -maßnahmen beschrieben. Desweiteren werden die bereits getroffenen Maßnahmen bewertet und mit der aktuellen Bedrohungslage sowie dem gegenwärtigen Stand der Technik abgeglichen. Abschließend werden Verbesserungen vorgeschlagen und bewertet.

2.1 Gefährdungslage

Die Gefährdungslage beschreibt die Gefährdung eines IT-Systems. Sie basiert unter anderem auf der Sicherheitslage der eingesetzten Software (Alter, Update-Status, Verfügbarkeit von Updates, Bekannte Sicherheitslücken) sowie weiteren Sicherheitsmaßnahmen (Zwei-Faktor-Authentifikation, Kryptographie) sowie Physikalischer Zugriffs- und Zutrittsschutz (gesichertes Rechenzentrum, Serverraum, Büro mit Publikumsverkehr).

Desweiteren wird die Eintrittswahrscheinlichkeit eines Schadensereignisses betrachtet. Ein öffentlich zugänglicher Server (Webserver, Mailserver) ist mit einer höheren Eintrittswahrscheinlichkeit gefährdet, als ein interner Firmen-Rechner hinter einer Firewall. Ein Laptop kann schneller gestohlen werden als ein Server.

Die Gefährdungslage ist in die 3 Stufen niedrig, mittel und hoch eingeteilt.

2.2 Schadenspotenzial

Das Schadenspotenzial beschreibt die Konsequenzen die ein Schadensfall für das Unternehmen hat. Dies kann wirtschaftlicher Natur sein (Umsatzverlust durch Ausfall eines Systems, Verlust von Reputation und Vertrauen) oder strafrechtlich relevant (Bußgelder oder Stilllegung von IT-Systemen durch die Aufsichtsbehörde für Datenschutz, Freiheitsstrafen gemäß §203 StGB »Verletzung von Privatgeheimnissen«)

Das Schadenspotenzial ist in die 4 Stufen niedrig, mittel, hoch, und sehr hoch unterteilt.

Wobei die Stufe *hoch* mit erheblichen Kosten für das Unternehmen verbunden ist und die Stufe *sehr hoch* die Existenz des Unternehmens bedroht ist und/oder Freiheitsstrafen bzw. empfindliche Geldstrafen drohen.

Die Einstufungen hoch und sehr hoch implizieren sofortige Maßnahmen mit hoher Priorität durch das Unternehmen.

2.3 Sicherheitsmaßnahmen

Die bisherigen Sicherheitsmaßnahmen werden basierend auf dem Schadenspotenzial, der Gefährdungslage und dem Schutzbedarf bewertet. Es werden die 3

Stufen sehr schlecht, ausreichend sowie sehr gut verwendet. Die Stufe *sehr schlecht* setzt dabei sofortige Maßnahmen mit hoher Priorität voraus.

2.4 Schutzbedarf

Der Schutzbedarf beschreibt den Bedarf an Schutzmaßnahmen die ein System erfordert. Es leitet sich ab aus gesetzlichen Forderungen bspw. aus dem Bundesdatenschutzgesetz bei der Verarbeitung von personenbezogenen Daten sowie aus ökonomischen Überlegungen, d.h. einer finanziellen Bewertung des Systems und der darauf befindlichen Daten. Ebenso werden die Konsequenzen bei Verlust bzw. Diebstahl der Daten oder Ausfall der Systeme betrachtet.

Systeme, die personenbezogende Daten verarbeiten, unterliegen dabei automatisch immer mindestens dem Schutzbedarf hoch.

Die Schutzbedarfsfeststellung kann genutzt werden, um den finanziellen Aufwand zur Sicherung eines Systems zu rechtfertigen bzw. abzuschätzen.

Der Schutzbedarf wird in den 3 Stufen normal,hoch und sehr hoch klassifiziert.

Eine weitere Unterteilung in die Eigenschaften *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* ist möglich.

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Daten dürfen lediglich von autorisierten Benutzern gelesen bzw. modifiziert werden, dies gilt für gespeicherte Daten wie für Übertragungswege.

Integrität Daten dürfen nicht unbemerkt verändert werden. Alle Änderungen müssen nachvollziehbar sein.

Verfügbarkeit Verhinderung von Systemausfällen; der Zugriff auf Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet sein.

Authentizität bezeichnet die Eigenschaften der Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit eines Objekts. Inhalte/Daten sind nicht verändert.

2.5 Prozess-Diagramm

Das Prozess-Diagramm visualisiert die Prozesse und IT im Unternehmen gemäß Emfehlung des BSIs zu Risikoanalysen. Dazu werden folgende Elemente dargestellt:

Komponenten sind Hardwarekomponenten, die können einzelne Rechner, Drucker oder externe Festplatten sein.

VM Virtuelle Maschinen die auf einer zugeordneten Hardwarekomponente laufen.

Anwendungen sind Programme die auf einer VM und/oder Komponente laufen und Funktionen oder Dienste bereitstellen.

Teilprozesse sind Teile eines Geschäftsprozesses.

Prozesse sind die Geschäftsprozesse oder technischen Prozesse im Unternehmen, bspw. die Umsatzsteuervoranmeldung, Vertrieb oder der Zugang zum Unternehmensnetz per VPN sowie die Anmeldung im Active Directory. Sie können aus mehreren Teilprozessen bestehen.

OrgEinheit ist die für einen Geschäftsprozess verantwortliche oder von einem technischen Prozess betroffene Organisationseinheit. Die Organisationseinheiten entsprechen dem Organigramm des Unternehmens erweitert um die OE *Alle*, wenn alle OE/Mitarbeiter betroffen sind, bspw. im Prozess Login und Anmeldung am Active Directory.

Durch die Visualisierung der Prozesse werden zum einen die relevanten Geschäftsprozesse identifiziert und die dazugehörige IT-Infrastruktur dargestellt. Daraus kann dann u.a. die Kritikalität bzw. der Schutzbedarf für die eingebundenen Komponenten, VMs und Anwendungen abgeschätzt werden. Desweiteren ist auf einen Blick ersichtlich, welche Prozesse gefährdet sind, wenn eine Komponente ausfällt.

Desweiteren bietet das Diagramm eine Entscheidungshilfe für die Geschäftsführung im Bereich Investition/TCO/ROI für Sicherheitsmaßnahmen an, da die Wichtigkeit der einzelnen Komponenten und Anwendungen einfacher abgeschätzt werden kann und eine Abhängigkeit des Unternehmens von einzelnen Prozessen und Komponenten leichter ersichtlich ist.

Im Verbund mit der restlichen Risikoanalyse, insbesondere der anfallenden Daten, wird das Prozessdiagramm genutzt um Risikopotenziale und Schutzmaßnahmen zu bestimmen.

Weitere Informationen zur Risikoanalyse und -bewertung finden Sie in (Bundesamt für Sicherheit in der Informationstechnik, 2005a, 2005b, 2008a, 2008b, 2011)

3 Was ist Sicherheit eigentlich und welche Angriffsrisiken existieren?

Sicherheit lässt sich auf verschiedene Arten definieren, so gibt es unter anderem DIN-Normen zur Elektrosicherheit oder zum Design von Maschinen, damit sich Bediener nicht an Ihnen verletzen können.

In der Informatik verwendet man in der Regel die VIVA-Kriterien zur Definition von Sicherheit.

In der Informatik bzw. der IT-Sicherheit werden verschiedene Diagnosekriterien festgelegt, die der Sicherheitsdiagnose von Software, Hardware und ganzen IT-Systemen dienen. Am bekanntesten sind die sogenannten VIVA-Kriterien, also Vertraulichkeit, Verfügbarkeit, Integrität und Authentisierung, welche unter anderem vom Bundesamt für Sicherheit in der Informationstechnik (2006) wie folgt definiert werden:

Vertraulichkeit Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.

Integrität Die Daten sind vollständig und unverändert. Der Begriff »Information» wird in der Informationstechnik für »Daten« verwendet, denen je

nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert wurden oder Angaben zum Autor verfälscht wurden oder der Zeitpunkt der Erstellung manipuliert wurde.

Verfügbarkeit Dem Benutzer stehen Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen zum geforderten Zeitpunkt zur Verfügung.

Authentisierung Bei der Anmeldung an einem System wird im Rahmen der Authentisierung die Identität der Person, die sich anmeldet, geprüft und verifiziert. Der Begriff wird auch verwendet, wenn die Identität von IT-Komponenten oder Anwendungen geprüft wird. Ist die Authentisierung erfolgreich, spricht man auch davon, dass die Person oder ein Datum authentisch ist bzw. die Authentizität gewährleistet ist.

Wenn Sie sich fragen, ob ein System sicher ist, überprüfen Sie ob es den VIVA-Kriterien genügt. Im folgenden ein Beispiel zur Sicherheit von E-Mails:

Vertraulichkeit E-Mails werden als einfache Textdatei zwischen den Mailservern weitergeleitet. Jeder der Zugriff auf die Mailqueue hat, kann die E-Mails auf einem Server lesen. Ebenso kann der Netzwerkverkehr an zentraler Stelle abgefangen und ausgewertet werden. Eine E-Mail ist also nicht vertraulich.

Integrität Jeder der schreibenden Zugriff auf die Mailqueue eines Mailservers hat, kann dort eine Mail verändern. Eine E-Mail ist also nicht integer.

Verfügbarkeit E-Mails können im Netz abgefangen werden und erreichen den Empfänger daher nicht. Die Verfügbarkeit von E-Mails ist nur eingeschränkt möglich.

Authentizität Zusammem mit der Integrität kann auch die Authentizität manipuliert werden, das heißt ein Angreifer kann nicht nur den Inhalt der Mail, sondern auch Absender und Zeitstempel ändern. Die Authentizität einer E-Mail ist daher nicht gewährleistet.

E-Mails sind also weder vertraulich, noch ist deren Integrität oder Authentizität gewährleistet. Dazu sind weitere Maßnahmen erforderlich, die wir später noch besprechen werden.

Ein möglicher Angriff auf eine E-Mail ist eine sogenannte Man-in-the-Middle-Attacke. Dabei handelt es sich um einen Angriff auf die Übertragung von Daten zwischen zwei Systemen oder auch zwei Programmen auf dem selben Computer. Der Angreifer plaziert sich dabei in der Mitte zwischen den beiden Kommunikationspartnern. Dies kann beispielsweise ein Mailserver beim Mailversand sein. Der Administrator des Mailservers eines Internetanbieters verfügt über alle Zugriffsrechte auf dem System und kann daher auch beliebig Mails lesen, löschen oder verändern.

Ein derartiger Angriff ist auf jede Form der elektronischen Datenübertragung möglich, egal ob es sich um eine Mail, den Login auf einer Webseite oder um ein Fax oder Telefonat handelt. Um die Übertragung abzusichern, ist der Einsatz von Verschlüsselung zwingend erforderlich.

Abb. 1 zeigt eine Man-in-the-Middle-Attacke auf die Kommunikation zwischen Alice und Bob.

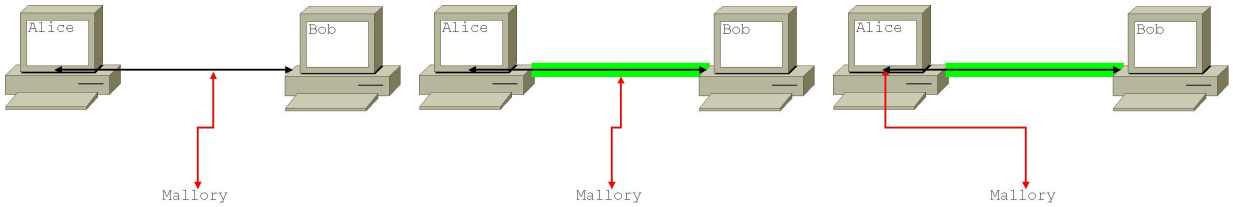
Ein weiteres Grundprinzip der IT-Sicherheit ist das sogenannte Schalen- oder Schichtenmodell. Ähnlich einer Zwiebel verfügen Betriebssysteme über mehrere Schalen. Jede Schale verfügt über bestimmte Berechtigungen im System, wobei die innerste Schale über sämtliche Berechtigungen und die äußerste über stark eingeschränkte Berechtigungen verfügt. Normalerweise läuft eine Anwendung auf der äußersten Schale und hat somit keinerlei Berechtigungen. Startet ein Anwender nun ein Programm für Videokonferenzen, möchte das Programm u.a. auf die Webcam und das Mikrofon zugreifen. Dazu muss es den Betriebssystemkern in inneren Schalenbereich um die entsprechenden Berechtigungen bitten. Erteilt das Betriebssystem diese Berechtigungen kann das Programm auf die Webcam und das Mikro zugreifen. Erhält es diese Berechtigung nicht, kann es die Hardware auch nicht nutzen.

Der Betriebssystemkern entscheidet daher ob eine Anwendung auf bestimmte Hardware, Dateien oder Prozesse zugreifen kann, dazu nutzt es unter anderem die Berechtigungen des ausführenden Benutzers. Das führt dazu, dass der Systemadministrator über alle Berechtigungen verfügt und daher auf jede Datei und jeden Prozess zugreifen darf.

Möchte ein Angreifer nun einen Rechner übernehmen ist es oberstes Ziel in den inneren Schalenbereich vorzudringen. Dies ermöglicht ihm unter anderem neue Benutzerkonten einzurichten und sich vor dem echten Systemadministrator zu verstecken. Hat ein Angreifer einen derartigen Zugriff erreicht, kann er sich auch vor Sicherheitssoftware verstecken. Damit kann sich auch eine Schadsoftware vor einem Virenscanner verstecken – um alle Dateien öffnen und scannen zu können, benötigt der Virenscanner Zugriffsrechte im Betriebssystemkern. Hat der Angreifer die Kontrolle über den Kern erreicht kann er diese Rechte nutzen um Dateien vor dem Virenscanner zu verstecken oder dem Virenscanner eine falsche Version der Datei vorlegen, die keinen Virus enthält. Virenscanner lassen sich damit technisch gesehen relativ simpel umgehen. Ein Systemadministrator oder Anwender kann sich daher auch nie sicher sein, dass der Computer wirklich frei von Schadsoftware ist.

4 Penetration Testing: Einbrechen wie die Hacker

Da es nicht möglich ist die Sicherheit eines Systems positivistisch zu beweisen, sind sogenannte Penetration Tests oder PenTests erfoderlich. Die Grundidee eines PenTests ist es, die Ziel-Infrastruktur ebenso anzugreifen, wie dies ein Hacker tun würde.



(a) Mallory kann die unverschlüsselte Kommunikation abfangen und verändern

(b) Lösung: Verschlüsselung zwischen den Endpunkten ermöglicht Authentifikation und Vertraulichkeit

(c) abschöpfen der Daten auf dem Zielsystem selbst, bevor diese verschlüsselt werden

Abbildung 1: Verschlüsselte und Unverschlüsselte Kommunikation

Dabei ist der PenTest vom Einsatz eines sogenannten Vulnerability Scanners zu unterscheiden. Es existieren für verschiedene Einsatzszenarien vorgefertigte Programme, die die Zielsysteme automatisiert auf bekannte Schwachstellen hin untersuchen.

Die bekanntesten Vulnerability Scanner sind OpenVAS, der Open-Source-Nachfolger von Nessus sowie der Microsoft Baseline Security Analyzer (MBSA). Der MBSA kann in Microsoft-Netzen dazu genutzt werden, die laufenden Rechner bezüglich der installierten Service Packs, Patches und Updates zu überprüfen.

Ein PenTest hingegen greift im Idealfall die gesamte Infrastruktur des Unternehmens als Black-Box-Analyse an. Das heißt dass ein spezialisierter Dienstleister von außen versucht in die Infrastruktur einzudringen und dort vordefinierte Ziele zu erreichen. So kann der Auftrag beispielsweise lauten bestimmte Dateien von einem Server zu kopieren, Dateien hochzuladen oder ein Rootkit auf einem Server zu installieren und einen APT einzurichten.

Neben der Technik kann auch die Organisation bzw. die Mitarbeiter mittels Social Engineering angegriffen werden. Ein PenTester könnte also auch versuchen in ein bestimmtes Büro einzudringen und dort einen Aktenordner zu entwenden oder per Telefonat versuchen das Passwort für den Geschäftsbankenzugang von einer Buchhalterin zu erlangen.

Der PenTest dient dazu, Schwachstellen und Bedienfehler zu finden, die technische Sicherheit zu erhöhen sowie die Sicherheitsorganisation zu verbessern.

Ein PenTest unterteilt sich dabei immer in die folgenden Phasen mit den entsprechenden Zielen und Aufgaben:

1. **Vorbereitung:** Ziele definieren, Vorgehensweise, Kontaktpersonen, Black/White List, Compliance
2. **Informationen sammeln und auswerten:** Details über Ziele, Google, Scanner, MetaSploit, Angriffsvektoren, Karte des Netzwerks erstellen
3. **Risikoanalyse:** Angriffspotential aus Schwachstellen errechnen,
4. **Einbruchsversuche:** Vulnerabilities exploiten, Beobachtung der Systeme sicherstellen
5. **Abschlussbericht:** Aufbereitung und Auswertung des Pen-Tests, der Logs etc.

Weitere Informationen zu PenTests finden Sie in Kohl (2012).

5 Social Engineering

Social-Engineering ist eine Angriffsstrategie, die auf eine psychologische Manipulation von Menschen abzielt. Dabei versucht der Angreifer, fundamentale menschliche Verhaltensweisen auszunutzen, um Zugriff auf sensible Daten zu bekommen.

Neben bekannten Beispielen von Social-Engineering-Attacken, wie dem berühmt-berüchtigten „Hauptmann von Köpenick“, beschreiben auch Mitnick und Simon (2006) sehr detailliert verschieden Angriffe, die Social-Engineering einsetzen. Der Autor war in den 1990er Jahren einer der am meisten gefürchteten Hacker in Amerika. Im Buch beschreibt er zahlreiche Angriffsmethoden, die nur zum Teil oder sogar keine technischen Hintergründe haben. Sein Beispiel handelt davon, dass ein kleines amerikanisches Ingenieurbüro eine neue Antriebstechnik für Hubschrauber entwickelt hat. Ein Konkurrent möchte diese Technik stehlen und setzt dazu Social-Engineering-Techniken ein.

Durch eine Meldung auf der Webseite bringt der Angreifer in Erfahrung, dass „John Smith“, der Chef des Ingenieurbüros auf einer Flugschau in Paris weilt, also ein paar Tage nicht verfügbar sein wird. In dieser Zeit mietet der Angreifer eine teure Limousine samt Chauffeur, außerdem kauft er sich teure Kleidung und eine teure Uhr und lässt sich professionell frisieren. Er möchte den Eindruck eines gut bezahlten (und wichtigen) Managers machen, idem er den für Manager üblichen Stil und das Verhalten kopiert. Er lässt sich beim Ingenieurbüro vorfahren und stellt sich am Empfang als „Bob“ von Boeing vor, der die Handbücher abholen möchte, die Johnny ihm versprochen hat.

Der Empfang weiß natürlich von nichts und blockt Bob zunächst ab. Dieser legt daraufhin seine „gefälschte“ Visitenkarte von Boeing vor und stellt sich als leitender Entwicklungsingenieur vor. Er habe „Johnny“, den Chef, auf einer Flugschau getroffen und sich mit ihm über die neue Antriebstechnik unterhalten. Inzwischen sei man sich handelseinig geworden, Bob habe die Technik bei Boeing vorgestellt und Boeing möchte sie nun für sehr viel Geld kaufen. Allerdings benötigt Bob dringend, am besten sofort, die technischen Handbücher, da er noch einige Kritiker bei Boeing überzeugen muss.

Die Empfangsdame ist erstaunt und erfreut, schließlich hat Bob ihrer Firma ein erfreuliches Angebot un-

terbreitet. Daher leitet sie Bob an den stellvertretenden Chef weiter. Diesem erzählt Bob die gleiche Geschichte und bittet darum, möglichst sofort die Handbücher zu bekommen. Da der stellvertretende Chef John wegen der Zeitverschiebung nach Europa nicht sofort erreichen kann, ist Bob verstimmt und droht damit, dass Geschäft platzen zu lassen. Nach einigem Hin und Her übergibt der Stellvertreter Bob die Handbücher. Einige Wochen später patentierte der Konkurrent die Technik, einige Monate später ging das Angriffsopfer in Konkurs.

Dieses Beispiel nutzt mehrere Social-Engineering-Techniken aus. Der Angreifer informiert sich auf der Webseite des Unternehmens darüber, das der Chef in Europa weilt und daher zumindest telefonisch nicht sofort erreichbar ist. Dann verkleidet er sich als Top-Manager und authentifiziert sich mit einer Visitenkarte, die man für ein paar Cent drucken lassen kann. Er macht der Firma ein lukratives Kaufangebot, zieht es aber später wieder zurück, als er die Handbücher nicht bekommen soll. Dadurch setzt er den stellvertretenden Chef unter Druck. Außerdem spricht er von Johnny, gibt also vor, mit dem Chef auf einer eher jovialen Ebene zu verkehren.

Social-Engineering ist äußerst erfolgreich, wenn größere Organisationen wie Unternehmen, Behörden oder Universitäten angegriffen werden sollen. Oftmals gelingt es einem Angreifer mit der Aggregation öffentlich zugänglicher Informationen und entsprechender Kaltschnäuzigkeit wichtige Informationen und Zugriff auf geschützte Systeme zu erlangen (vgl. Brack, 2017).

Die Motivation für einen Angriff kann unterschiedlich sein, neben „professionellen“ Gründen wie Industriespionage oder Identitätsdiebstahl kommen auch soziale Gründe wie Rache (z. B. durch Ex-Mitarbeiter) oder Spaß und Machtgefühl in Frage.

Eine weitverbreitete und bekannte Masche des Social-Engineering ist das sogenannte Phishing, bei dem mit gefälschten Emails oder Webseiten Benutzer dazu verleitet werden sollen, Logindaten zu ihren Bank- oder Emailkonten anzugeben. Derartige Angriffe sind sehr leicht durchzuführen, da man dazu lediglich etwas Webspace benötigt und dort die entsprechende Webseite nachahmt. Leider fallen immer wieder viele Benutzer auch auf holprige Emails mit Stilblüten wie „Zu der Beachtung!“ – eine wortwörtliche Übersetzung des englischen „To the Attention!“ – herein und offenbaren ihre Bankdaten.

Social Engineering Angriffe sind äußerst effektiv. Schutzmaßnahmen dagegen müssen immer Schulungen und Trainings der Mitarbeiter beinhalten. Es handelt sich hierbei um ein Soziales Problem, für das keine technische Lösung existiert (Schumacher, 2010, 2014c, 2015a, 2015b, 2018).

Literatur

Brack, D. C. (2017). Social Engineering - The Most Underestimated APT: Hacking the Human Operating System. Verfügbar 18. September 2017 unter http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS_056_Brack_SEET.pdf

Brack, D. C. (2019). Drones, the New Threat from the Sky. *Magdeburger Journal zur Sicherheitsforschung*, *18*, 969–976. Verfügbar 17. Oktober 2019 unter http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS_067_Brack_Drones.pdf

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.). (2005a). BSI-Standard 100-3: Risikoanalyse auf Basis von IT-Grundschutz.

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.). (2005b). Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT.

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.). (2006). Leitfaden IT-Sicherheit IT-Grundschutz kompakt. Verfügbar 16. Oktober 2006 unter http://www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.). (2008a). BSI-Standard 100-1: Managementsysteme für Informationssicherheit.

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.). (2008b). BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise.

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.). (2011). BSI-Standard 100-4:Die IT-Notfallplanung als Element der IT-Sicherheit.

Chebbi, C. (2018). Malware Analysis: Machine Learning Approaches. *Magdeburger Journal zur Sicherheitsforschung*, *16*, 893–899. Verfügbar 17. November 2018 unter http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS_060_Chebbi_MachineLearning.pdf

Feyrer, H. (2012). Eine DIN für IT-Sicherheit? *Magdeburger Journal zur Sicherheitsforschung*, *4*, 323–342. Verfügbar 16. Dezember 2012 unter http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS-020.pdf

Feyrer, H. (2018). Was ist Informationssicherheit? Positionierung, Chancen und Risiken. *Magdeburger Journal zur Sicherheitsforschung*, *15*, 871–878. Verfügbar 19. Februar 2018 unter http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS_058_Feyrer_Sicherheit.pdf

Fischer, T. (2018). I Wrote my Own Ransomware; did not make 1 iota of a Bitcoin. *Magdeburger Journal zur Sicherheitsforschung*, *16*, 879–892. Verfügbar 3. November 2018 unter http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS_059_Fischer_Ransomware.pdf

Holtmanns, S. (2019). New Attack Vectors for Mobile Core Networks. *Magdeburger Journal zur Sicherheitsforschung*, *18*, 943–951. Verfügbar 5. August 2019 unter http://www.sicherheitsforschung-magdeburg.de/

uploads / journal / MJS _ 064 _ Holtmanns _ MobileCoreNetworks.pdf

Kafka, M. & Pfeiffer, R. (2012). Angriffe und Verteidigungsstrategien für vertrauliche Kommunikation über Funkdienste. *Magdeburger Journal zur Sicherheitsforschung*, *4*, 308–322. Verfügbar 13. Dezember 2012 unter http : / / www.sicherheitsforschung-magdeburg.de / uploads/journal/MJS-019.pdf

Kohl, M. (2012). Penetrationstests mit Metasploit. In J. Sambleben & S. Schumacher (Hrsg.), *Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen?* (S. 137–152). Norderstedt, BoD.

Mitnick, K. & Simon, W. (2006). *Die Kunst des Einbruchs* (1. Aufl.). Heidelberg, MITP.

Schumacher, S. (2010). Psychologische Grundlagen des Social-Engineering (Chaos Computer Club, Hrsg.). *Die Datenschleuder: Das wissenschaftliche Fachblatt für den Datenreisenden*, *#94*, 52–59. Verfügbar 10. Oktober 2010 unter http://ds.ccc.de/pdfs/ds094.pdf

Schumacher, S. (2011). Sicherheit messen: Eine Operationalisierung als latentes soziales Konstrukt. In S. Adorf, J.-F. Schaffeld & D. Schössler (Hrsg.), *Die sicherheitspolitische Streitkultur in der Bundesrepublik Deutschland: Beiträge zum 1. akademischen Nachwuchsförderpreis Goldene Eule des Bundesverbandes Sicherheitspolitik an Hochschulen (BSH)* (S. 1–38). Magdeburg, Meine Verlag.

Schumacher, S. (2012a). Vom Cyber-Frieden. In J. Sambleben & S. Schumacher (Hrsg.), *Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen?* (S. 337–361). Norderstedt, BoD.

Schumacher, S. (2012b). Vom Cyber-Kriege. In J. Sambleben & S. Schumacher (Hrsg.), *Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen?* (S. 1–26). Norderstedt, BoD.

Schumacher, S. (2013). Soziale Kompetenzen für Informatiker. *UpTimes*, *3*, 18–28. Verfügbar 16. Dezember 2013 unter http://www.guug.de/uptimes/2013-3/index.html

Schumacher, S. (2014a). Cyber-Terrorismus: Reale Bedrohung oder Mythos? In S. Hansen & J. Krause (Hrsg.), *Jahrbuch Terrorismus 2013/2014* (S. 159–177). Opladen, Verlag Barbara Budrich.

Schumacher, S. (2014b). Das IT-Weiterbildungssystem und IT-Sicherheit. *Magdeburger Journal zur Sicherheitsforschung*, *7*, 456–467. Verfügbar 24. Juni 2014 unter http : / / www . sicherheitsforschung - magdeburg . de / uploads / journal / MJS - 030 - Schumacher - ITWeiterbildungssystem.pdf

Schumacher, S. (2014c). Psychologische Grundlagen des Social-Engineering. *Information: Wissenschaft und Praxis*, *65*, 215–230.

Schumacher, S. (2015a). Psychology of Security: A Research Programme. In S. Schumacher & R. Pfeiffer (Hrsg.), *In Depth Security: Proceedings of the DeepSec Conferences* (S. 169–180). Magdeburg, Magdeburger Institut für Sicherheitsforschung.

Schumacher, S. (2015b). Psychology of Security: A Research Programme. *Magdeburger Journal zur Sicherheitsforschung*, *10*, 667–674. Verfügbar 25. Oktober 2015 unter http : / / www . sicherheitsforschung - magdeburg . de / uploads / journal / MJS _ 041 _ SchumacherPsychology.pdf

Schumacher, S. (2017). Informationssicherheit in Versorgungsunternehmen umsetzen, In *22. Thüringer Wasserkolloquium*, Erfurt, Fachhochschule Erfurt.

Schumacher, S. (2018). Sicherheitsfaktor Mensch. *Managementkompass: Unternehmen schützen – Risiken minimieren*, 16–17.

Schumacher, S. (2020). Informationssicherheit in Versorgungsunternehmen umsetzen: Einige praktische Erfahrungen. *Magdeburger Journal zur Sicherheitsforschung*, *20*, 995–1002. Verfügbar 29. Dezember 2020 unter http : / / www.sicherheitsforschung-magdeburg.de / uploads / journal / MJS _ 070 _ Schumacher _ Versorgungsunternehmen.pdf

Seidler, F. F. (2012). Sicherheitsumfeld Cyber-Space: Abhängigkeiten, Akteure, Herausforderungen und Perspektiven. In J. Sambleben & S. Schumacher (Hrsg.), *Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen?* (S. 215–228). Norderstedt, BoD.

Shukla, P. (2015). The Compromised Devices of the Carna Botnet: As used for the Internet Census 2012. *Magdeburger Journal zur Sicherheitsforschung*, *10*, 547–627. Verfügbar 22. Oktober 2015 unter http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS_038_Shukla_Carna.pdf

Slowik, J. (2019). Defense Informs Offense Improves Defense: How to Compromise an Industrial Control Systems Network – and How to Defend it. *Magdeburger Journal zur Sicherheitsforschung*, *18*, 960–968. Verfügbar 15. September 2019 unter http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS_066_Slowik_ICS.pdf

Weiße, G. K. (2012). Die Sicherheitsarchitektur der EU im Wandel: Die geplante parlamentarische Kontrolle der Sicherheits- und Nachrichtendienste in der Europäischen Union durch das Europa-Parlament. In J. Sambleben & S. Schumacher (Hrsg.), *Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen?* (S. 229–244). Norderstedt, BoD.