Life Is On | Schneider Electric

Gebäudemanagement-Systeme gegen Cyber-Gefahren schützen

von Daniel Paillet, CISSP, CEH

Zusammenfassung

Bis vor kurzem war die Sicherheitsüberwachung für Gebäudemanagement-Systeme (BMS) kein Thema. Aber angesichts wachsender Gefahren durch Cyberangriffe muss die Integrität dieser Systeme besser geschützt werden. Für Computer und Datacenter gibt es etablierte Monitoring-Verfahren, aber Gebäudemanagement-Systeme werden oft ignoriert. In diesem White Paper beschreiben wir die Gefahren und empfehlen Vorgehensweisen zur Implementierung einer „Defense-in-Depth"-Methode speziell für den Schutz von Gebäudemanagement-Systemen.

Einführung

Die Bedrohung durch Cyberangriffe auf Gebäudemanagement-Systeme (BMS) gewinnt innerhalb und außerhalb des Facility Managements immer mehr an Bedeutung. Bei einem Angriff auf den amerikanischen Handelsriesen Target (fast 1800 Kaufhäuser in den USA), der vor kurzem für Schlagzeilen sorgte, wurden 40 Millionen Kreditkartennummern innerhalb von 19 Tagen gestohlen. Ausgangspunkt für diese Datenschutzverletzung waren die Zugriffsrechte, die Target einem externen HLK-Unternehmen (Heizung, Lüftung und Klimatisierung) für sein Netzwerk eingeräumt hatte. Hacker bekamen damit einen Zugang, über den sie einen Angriff auf kritischere Systeme im Netzwerk von Target starten konnten.[1]

Gebäude- und Zugangskontrollsysteme nutzen Computer zur Überwachung und Steuerung der Gebäudetechnik wie Klimatisierung, Stromversorgung, elektronische Kartenleser, Aufzüge, Brandmelder und Brandschutz, Heizung, Beleuchtung, Lüftung und Videoüberwachung. Alle diese Komponenten werden zunehmend mit anderen Informationssystemen und dem Internet vernetzt. Diese fortschrittlichen Technologien treiben zwar die Automatisierung voran und ermöglichen den Fernbetrieb, bergen aber auch die Gefahr von Cyberangriffen. Beim Netzwerk der US-Regierung, das nahezu 9.000 Bundesbehörden verbindet, hatte sich bis vor kurzem niemand mit den möglichen Cyber-Risiken auseinandergesetzt. Diese Bedrohung galt immer noch als „Problem der Zukunft“. Ein Cyberexperte setzte deshalb Regierungsbehörden wie das Government Accountability Office (GAO) darüber in Kenntnis, dass in diese Systeme keinerlei Cybersicherheits-Mechanismen integriert sind.

Jetzt ist das amerikanische Heimatschutzministerium, das U.S. Department of Homeland Security (DHS), auf diese Gefahren aufmerksam geworden. In den Fiskaljahren 2011 bis 2014 stieg die Zahl von Cyber-Angriffen auf industrielle Steuersysteme, darunter auch Gebäude- und Zutrittskontrollsysteme, von 140 auf 243 – ein Sprung von 74%. Die Kosten für diese Schutzverletzungen belaufen sich auf Hunderte Milliarden US-Dollar pro Jahr. Eine internationale Strafverfolgungsbehörde geht davon aus, dass die Opfer dieser Angriffe jährlich einen Verlust von weltweit 400 Milliarden US-Dollar erleiden. Wir sprechen hier von einem größeren kriminellen Unterfangen als der globale Handel mit Marihuana, Kokain und Heroin zusammen.[2]

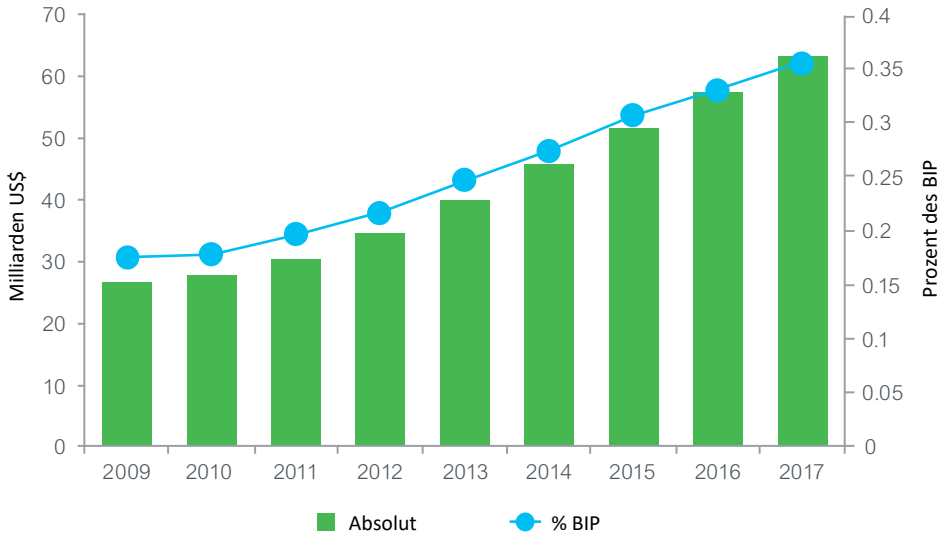

Abbildung 1

Anstieg der Ausgaben für Cybersicherheit in den USA (mit freundlicher Genehmigung der Telecommunications Industry Association).

[1] http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

[2] https://news.clearancejobs/01/26/dhs-eyes-cybersecurity-issues-building-control-systems/

Eine weitere Studie kommt zu einem ähnlichen Schluss. Darin werden die Kosten für Cyber-Angriffe weltweit auf 300 Milliarden bis 1 Billion US-Dollar geschätzt.[3] Zwar sind die finanziellen Folgen für Unternehmen je nach Land und Branche unterschiedlich, aber für alle gilt, dass die Kosten für Cyber-Angriffe jedes Jahr steigen.[4]

„Defense-in-Depth“ im Gebäude-management

Defense-in-Depth ist eine Datenschutzstrategie, die Menschen, Technologie und Betriebsabläufe integriert und mehrstufige Barrieren etabliert, um die kritischen Prozesse eines Unternehmens wirksam zu schützen.[5]

Obwohl Defense-in-Depth-Konzepte in der Regel in der Informationstechnologie (IT) angewendet werden, sollten sie auch in der Betriebstechnik (OT) und damit auch für Gebäudemanagement-Systeme (BMS) eingesetzt werden. Es besteht aber ein Unterschied, wie dieser Ansatz für OT bzw. IT implementiert wird. Bei IT-Systemen geht es in erster Linie um die drei Sicherheitskernbereiche Vertraulichkeit, Integrität und Verfügbarkeit von **Informationen** (in dieser Reihenfolge). Bei einem BMS sind diese drei Sicherheitsprioritäten erstens die Verfügbarkeit von Betriebseinrichtungen, zweitens die Integrität/Zuverlässigkeit der Betriebsprozesse und drittens die Vertraulichkeit von Betriebsinformationen.

Die Einführung eines solchen bereichsübergreifenden Abwehrmechanismus auf mehreren Systemebenen erfordert einen Kosten/Nutzen-Fokus auf den drei wichtigsten Ebenen: Menschen, Technik und Betrieb.[6] **Tabelle 1** zeigt die wichtigsten Maßnahmen, die auf jeder dieser Ebenen durchgeführt werden müssen.

Tabelle 1

Die wichtigsten Maßnahmen in diesen drei Sicherheitsbereichen.

Menschen	Technik	Betrieb
Unterstützung durch die Unternehmensführung	Beschaffung und Installation der erforderlichen Technik	Definition und Umsetzung von Routinemaßnahmen, die zur Gewährleistung der Betriebssicherheit erforderlich sind[7]
Schulung und Sensibilisierung der Mitarbeiter im Gebäudemanagement (und aller anderen Mitarbeiter mit Systemzugriff) hinsichtlich Cyber-Gefahren	Installation von Schutzmechanismen an mehreren Punkten	
Definition von Zuständigkeiten hinsichtlich Cyber-Schutz und Zuweisung entsprechender Rollen in der IT und im Gebäudemanagement	Mehrstufige Implementierung von Abwehrmechanismen, Isolierung/Einschränkung des Zugriffs auf das BMS über das IT-Netzwerk	
Festschreibung von Sicherheitsrichtlinien und -verfahren	Implementierung von Technologien zur Erkennung von Angriffen	

[3] http://oreo.schneider-electric.com/flipFlop/695962877/files/docs/all.pdf

[4] „Understanding the economics of IT risk and reputation“, IBM, November 2013.

[5] http://www.ncsc.gov/publications/policy/docs/CNSSI_4009.pdf

[6] https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

[7] https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

Bedrohungen gehen nicht nur von Hackern aus, die das Internet nach Sicherheitslücken durchsuchen. Auch interne Mitarbeiter und externe Dienstleister stellen eine Gefahr dar. Techniken, mit denen Menschen Systeme bedrohen, sind:

- Phishing – Betrüger geben sich als legitimes Unternehmen bzw. als Betreiber einer legitimen Website aus, um sich Zugang zu einem Online-Account mit Finanzinformationen zu erschleichen.
- Spear Phishing – Eine E-Mail, die von einem legitimen Unternehmen oder einer legitimen Person zu stammen scheint. Die E-Mail kommt aber tatsächlich von Kriminellen, die eine Kreditkartennummer, ein Passwort oder Finanzinformationen vom Rechner ihres Opfers stehlen möchten.
- Advance Persistent Threats (APT) – Netzwerkangriffe, bei denen sich ein Unbefugter Zugang zu einem bestimmten Netzwerk verschafft und über einen längeren Zeitraum unentdeckt im Netzwerk bleibt. APT-Angriffe zielen auf den Diebstahl von Unternehmensinformationen.

Mehr technologie-orientierte Bedrohungen sind:

- Malware – Schad-Code bzw. -Software zur Ausführung unautorisierter Aktionen auf einem Computersystem.
- Key Logger – Ein Programm, das Tastatureingaben auf einem Computer aufzeichnet und ein Protokoll davon erstellt. Das Protokoll wird dann über das Internet an den Angreifer geschickt, der die Software installiert hat.
- USB Key Drop – Ein USB-Stick, der auf Parkplätzen oder in Parkhäusern in der Hoffnung deponiert wird, dass ihn jemand mitnimmt und in einen Bürocomputer einsteckt. Der Stick kann Schadsoftware enthalten, Viren in den Rechner laden oder sogar Informationen vom infizierten PC über das Internet versenden.
- Pwnie Plug – Ein kleines Gerät, das wie ein Netzteil aussieht und in einer Steckdose eingesteckt ist. Tatsächlich dient es dazu, Netzwerke in der Nähe zu hacken.
- Pineapple – Ein batteriebetriebenes drahtloses Hacking-Gerät, das zum Angriff auf drahtlose Netzwerke bzw. Geräte genutzt werden kann.

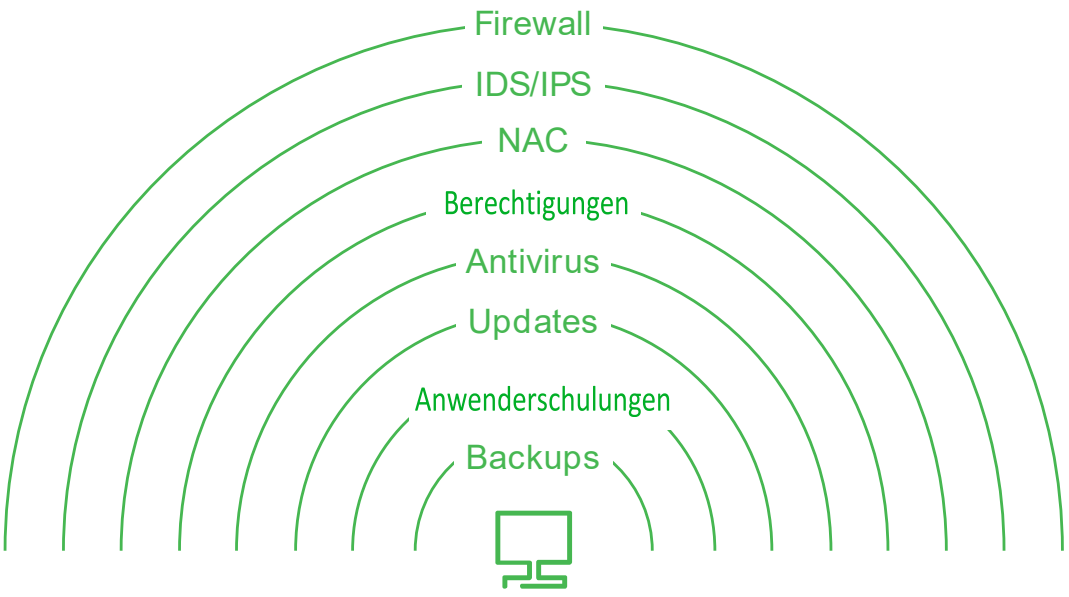

Abbildung 2

Beispiel für ein mehrstufiges Sicherheitskonzept

Der mehrstufige Schutzmechanismus in Abbildung 2 wurde vom United States Control Systems Security (CSSP) entwickelt. Diese beispielhafte Defense-in-Depth-Implementierung arbeitet mit unterschiedlichen Risikomanagement-Strategien. Wenn eine Schutzebene versagt, gibt es eine weitere Stufe zur Verhinderung einer umfassenden Datenschutzverletzung.[8]

Defense-in-Breadth

Defense-in-Breadth, eine Ergänzung der Defense-in-Depth-Methode, lässt sich wie folgt definieren: „Ein systematischer, bereichsübergreifender Maßnahmenkatalog für die Identifizierung, das Management und die Reduzierung von Risiken durch Schwachstellen in jeder Phase des System-, Netzwerk- oder Teilkomponenten-Lebenszyklus (System-, Netzwerk- oder Produkt-Design und -Entwicklung; Fertigung; Verpackung; Montage; Systemintegration; Distribution; Betrieb; Wartung; Außerbetriebnahme).[9] Kurz, Defense-in-Breadth arbeitet mit verschiedenen Arten von Sicherheitssystemen auf jeder Sicherheitsebene.“[10]

Der Unterschied zwischen Defense-in-Breadth und Defense-in-Depth lässt sich am besten anhand des folgenden Antivirus-Beispiels erklären: Defense-in-Depth nutzt ein bestimmtes Anti-Malware-Paket zur Gefahrenabwehr. Defense-in-Breadth arbeitet dagegen unter Umständen mit mehreren Anti-Malware-Anwendungen. Es empfiehlt sich, beide Ansätze zu implementieren, weil eine bestimmte Antivirus-Software ggfs. einen Virus erkennt, der einer anderen entgeht. Der Einsatz von Antiviren-Software eines Anbieters auf einem E-Mail-Server und die Verwendung der Tools eines anderen Anbieters auf PCs, Workstations und Servern spannt ein breiteres Sicherheitsnetz (in diesem Fall gegen Viren).

Bei Gebäudemanagement-Systemen zielt Defense-in-Depth/Breadth auf Gateways, Messgeräte und Steuerungen. Der Aufbau einer Sicherheitsarchitektur beginnt damit, dass der Hersteller dieser Komponenten einen Security Development Lifecycle bei der Produktion von Geräten und Software für Gebäudemanagement-Systeme befolgt (siehe Abbildung 3). Mit diesem Prozess zur Entwicklung „gehärteter“ (sicherheitsoptimierter) Geräte und Software können diese gegen Angriffe gesichert werden. Abbildung 3 zeigt die unterschiedlichen Ebenen und Prozesse für das Härten eines BMS, das die Merkmale Secure by Design (Sicherung durch Design), Secure by Default (Sicherung durch Standardeinstellungen) und Secure in Deployment (Sicherung durch optimierte Implementierung) aufweist.

Abbildung 3

Security Development Lifecycle.

[8]Viega und McGraw [Viega 02] in Kapitel 5, „Guiding Principles for Software Security“, in „Principle 2: Practice Defense in Depth“, Seiten 96-97

[9]http://www.ncsc.gov/publications/policy/docs/CNSSI_4009.pdf

[10]Official (ISC2) Guide to CISSP-ISSMP CBK, Second Edition, Seite 198

BMS-Sicherheit

Wenn es um Gebäudemanagement-Systeme (BMS) geht, muss ein Cybersicherheits-Konzept mehr Dinge erfassen als die allgemein bekannten, vorsätzlichen Angriffe von verärgerten Mitarbeitern, Industriespionen und/oder Terroristen. Gelegentlich können nämlich Anwenderfehler, Geräteausfälle oder Naturkatastrophen das System verwundbar machen. Die resultierenden Schwachstellen im Perimeterschutz kann dann ein Angreifer ausnutzen, um in das Netzwerk einzudringen, sich Zugriff auf Steuerungssoftware zu verschaffen und die Lastbedingungen zu ändern, um das System auf unkalkulierbare Art und Weise zu destabilisieren.[11]

Tabelle 2 zeigt, wie sich BMS-Netzwerke durch ein gezieltes Management der Sicherheitssystem-Prozesse und -Verfahren besser gegen Gefahren schützen lassen.

Tabelle 2
Best Practices zur Stärkung der BMS-Netzwerksicherheit

Prozesse	Verfahren	Vorteile
• Einhaltung von Standards und Vorschriften • Management von Anmeldedaten • Systemadministration • Patch-Management • Reaktion auf sicherheitsrelevante Ereignisse	• Mitarbeiterschulungen • Regelmäßige Beurteilungen	• Verhinderung der unbemerkten Einschleusung von Malware • Vermeidung von Datenschutzverletzungen durch Social Engineering • Einhaltung von Normen

Der Link in der Fußnote unten auf dieser Seite führt zu detaillierten Informationen zu den in Tabelle 2 aufgeführten Punkten.[12]

Zur Maximierung des Schutzes sollten konventionelle IT-Sicherheitslösungen in die BMS-Netzwerke eingebunden werden. Im Folgenden werden einige Bereiche aufgelistet, die im Sicherheits-Gesamtkonzept zu berücksichtigen sind:

Zugangskontrollen

- Physische Zugangskontrollen: Zäune, Sicherheitsschlösser, Kartenleser, Videokameras
- Kontrollen an den Netzwerkgrenzen: Firewalls, VPN, unidirektionale Gateways

Netzwerkhärtung

- Prozesse und Verfahren für die Installation von Software und eingebetteten Geräten beinhalten Dinge wie die Änderung von Standardberechtigungen und die Deaktivierung ungenutzter Services in Betriebssystemen
- Implementierung von Host Intrusion Prevention Systemen (HIPS) in Endpoints, „White Listing“ für Anwendungen (die Verwendung von Spamfiltersoftware, die nur E-Mails von bestimmten Adressen passieren lässt), um die Aktivierung von Trojanern und Schadsoftware auf Servern/Workstations zu unterbinden

[11]NIST Smart Interoperability Panel: Cyber Security Group

[12]http://iom.invensys.com/EN/pdfLibrary/NERCCIPComplianceChecklist.pdf

Authentifizierung und Autorisierung

- Zentrales Account-Management für die Authentifizierung und Autorisierung von Benutzern
- Rollenbasierte Zugangskontrollen und Endbenutzer-Berechtigungen
- Überwachung und Überprüfung von Systemereignissen
- Zentrale Sicherheitsereignisprotokollierung von Netzwerk- und Systemzugriffen
- IDS/IPS-Systeme (Intrusion Detection bzw. Intrusion Prevention Systeme) zur Erkennung von anormalem Datenverkehr auf dem Netzwerk
- Tool für das Management sicherheitsrelevanter Vorfälle mit Echtzeitalarmen und Überwachung rund um die Uhr

Die Verbesserung der Verfügbarkeit und Zuverlässigkeit des Netzwerks stärkt das Vertrauen der Kunden in die Cyberschutz-Funktionalität des BMS.

Das amerikanische National Institute of Standards and Technology (NIST) hat Leitlinien für die Entwicklung eines Frameworks zur Verbesserung der Cybersicherheit von Gebäudemanagement-Systemen herausgegeben. Eines dieser Dokumente, *„Framework for Improving Critical Infrastructure Cyber Security“,* beschreibt die Grundprinzipien für die Implementierung eines Frameworks. Mit einem Framework, so NIST, kann ein Unternehmen – unabhängig von seiner Größe, seines Cybersicherheits-Risikos oder seiner Cybersicherheits-Kompetenz – die Prinzipien und Best Practices für das Risikomanagement zur Optimierung der Sicherheit und Resilienz seiner kritischen Infrastruktur anwenden. Das Framework umfasst eine Zusammenstellung praxisbewährter Standards, Richtlinien und Vorgehensweisen, die eine strukturierte Grundlage für die Umsetzung verschiedener Cybersicherheits-Ansätze schafft. Es sollte international anerkannte Standards für Cybersicherheit beinhalten. Die Unternehmen können das Framework auf globaler Ebene verwenden. Zudem kann es als Modell für die internationale Zusammenarbeit zur Erhöhung der Cybersicherheit kritischer Infrastrukturen dienen.[13]

Das schwächste Glied in jeder IT- oder Gebäudemanagement-Installation sind die Administratoren und Benutzer der Systeme. Ihre Handlungen können die Sicherheitsrisiken absichtlich oder unabsichtlich erhöhen. Zu den unbeabsichtigt herbeigeführten Gefahren zählen ungesicherte Laptops, Workstations und Arbeitsbereiche oder Verstöße gegen die vorgeschriebenen Prozesse und Verfahren (beispielsweise beim Passwortmanagement, wenn die Zugangsdaten und Zugriffsrechte eines Mitarbeiters, der das Unternehmen verlässt, nicht gelöscht werden). Absichtlich herbeigeführte Gefahren sind u.a. Sabotage, Betrug, Diebstahl oder die Weitergabe von Intellectual Property oder von geheimen/vertraulichen Informationen durch Insider.

Bedrohung durch „Social Engineering“

Im Zusammenhang mit Cybersicherheit bezeichnet Social Engineering eine Person, die eine andere Person, die einen Computer besitzt (oder internen Zugriff auf bestimmte Netzwerke und/oder Datenbanken hat) so manipuliert, dass diese unter falschen Vorwänden die Anweisungen des Täters befolgt. Beispielsweise könnte sich ein Anrufer als Mitarbeiter des IT-Supports ausgeben und nach Zugangsdaten oder anderen vertraulichen Informationen fragen. Weitere Beispiele für diese Art von Angriffen werden im Folgenden detailliert beschrieben.

Beispiel 1: E-Mail an einen „Freund“

Der Benutzer glaubt, dass er eine legitime E-Mail von einem Freund erhalten hat. Wenn sich ein Betrüger das E-Mail-Passwort einer Person durch Hacking oder Social Engineering verschafft hat, kann er aller Wahrscheinlichkeit nach auf die Kontaktliste seines Opfers zugreifen. Das ist deshalb der Fall, weil die meisten Menschen nur ein Passwort für viele Anwendungen nutzen. Das heißt, der Kriminelle hat höchstwahrscheinlich Zugang zu den sozialen Netzwerk-Kontakten des Opfers.

[13] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Sobald der Kriminelle sich die Kontrolle über dieses E-Mail-Account verschafft hat, verschickt er Mails an alle Kontakte des Betroffenen oder postet Nachrichten auf allen sozialen Netzwerken aller seiner Freunde und unter Umständen der Freunde dieser Freunde.

Die Nachrichten des Hackers zielen darauf, Vertrauen und Neugier zu erwecken. Sie enthalten beispielsweise einen Link mit der Aufforderung „Das musst Du Dir unbedingt ansehen!“. Da der Link von einem Freund kommt und die Empfänger neugierig sind, vertrauen sie dem Link und klicken darauf. Die Folge ist eine Malware-Infektion, und der Täter kann die Kontrolle über den Rechner übernehmen und die Kontaktinformationen stehlen, um dann diese Kontakte genauso zu täuschen, wie sein ursprüngliches Opfer.

In anderen Fällen enthält die E-Mail einen Button zum Download von Bildern, Musik, einem Film oder einem Dokument mit integrierter Malware. Sobald der Download gestartet wird – was wahrscheinlich passiert, weil die Mail ja angeblich von einem Freund kommt – wird der Rechner des Mail-Empfängers infiziert. Jetzt hat der Kriminelle Zugriff auf diesen Computer, auf das E-Mail-Account sowie auf die Social-Network-Accounts und -Kontaktdaten und er kann seinen Angriff auf alle diese Kontakte erweitern.

Die Nachrichten, die der Hacker verschickt, enthalten häufig eine überzeugende Geschichte oder einen plausiblen Vorwand. Beispielsweise erhält der Empfänger eine dringende Bitte von seinem „Freund“ um Hilfe, weil er nach einem Überfall irgendwo festsitzt und jetzt unbedingt Geld braucht, um wieder nach Hause zu kommen. Oder der Adressat wird um eine Spende für einen wohltätigen Zweck oder für eine andere wichtige Angelegenheit gebeten – zusammen mit einer Anleitung zur Überweisung des Geldes (an den Kriminellen).

Beispiel 2: Phishing-Versuch

Ein Hacker, der einen Phishing-Versuch unternimmt, verschickt eine E-Mail, eine Sofortnachricht oder eine SMS, die scheinbar von einer allgemein bekannten Firma, Bank, Schule oder Institution kommt. In der Regel präsentieren diese Nachrichten dem Empfänger eine Szenario oder Geschichte. Dabei wird beispielsweise ein Problem beschrieben, das vom Adressaten die „Bestätigung“ von Informationen erfordert, indem er auf den angezeigten Link klickt und Angaben in ein Formular einträgt. Die verlinkte Website sieht meistens ganz offiziell aus und weist auch die richtigen Logos und plausible Inhalte auf (der Betrüger hat nämlich das Format und den Content der echten Website unter Umständen eins zu eins kopiert). Da alles legitim erscheint, vertraut der Empfänger der Mail und der gefälschten Website und gibt die Informationen preis, die der Kriminelle abfragt. Diese Art von Phishing-Betrug arbeitet oft mit einer Warnung vor den möglichen Folgen, wenn der Empfänger nicht sofort handelt. Die Täter wissen nämlich, dass der Adressat wahrscheinlicher auf den Betrug hereinfällt, wenn er handelt, bevor er denkt.

Die Nachricht enthält oft auch einen „Glückwunsch, Sie haben gewonnen“. In der E-Mail wird behauptet, sie stamme von einem Veranstalter eines Gewinnspiels oder der Empfänger sei der Millionste Besucher der Site. Um den „Gewinn“ zu übermitteln, wird der Empfänger nach seiner Bankverbindung oder Adresse und Telefonnummer gefragt. Zudem wird er auch um einen Identitätsnachweis gebeten. Dabei handelt es sich um „Greed-Phishing“, das mit der menschlichen Gier spielt. Oft ist die vorgegebene Geschichte zwar sehr fadenscheinig, aber die Empfänger möchten gerne das haben, was ihnen vorgespiegelt wird, und fallen auf den Betrug herein. Sie geben ihre Informationen preis und müssen dann feststellen, dass ihr Konto leergeräumt oder ihre Identität gestohlen wurde.

Beispiel 3: „Baiting“-Tricks

Diese Social-Engineering-Tricks nutzen den Wunsch der Menschen aus, ein „Schnäppchen“ zu machen. Der Köder („Bait“) kann ein guter Preis für einen bestimmten Artikel oder ein toller neuer Film oder Song sein. Diese Tricks sind oft auf Peer-to-Peer-Sites, in sozialen Netzwerken oder auf betrügerischen Websites zu finden, die in einer Liste von Suchergebnissen erscheinen. Der Betrug tarnt sich oft auch als überaus gutes Angebot, das auf Werbe- oder Auktions-Sites angezeigt wird. Um keinen Verdacht aufkommen zu lassen, werden gute Ratings für den Verkäufer angezeigt (alles vorher so geplant und arrangiert). Die Rechner der Benutzer, die auf diesen Trick hereinfallen, werden unter Umständen mit Malware infiziert, die neue Angriffe gegen ihn und seine Kontakte startet. Sie verlieren vielleicht ihr Geld, ohne den gekauften Artikel zu erhalten. Wenn sie unvorsichtigerweise ihre Bankdaten preisgegeben haben, wird unter Umständen auch noch ihr Konto leergeräumt.

Beispiel 4: Antwort auf eine Frage, die der Benutzer nie gestellt hat

Kriminelle geben vor, auf eine „Bitte um Hilfe“ bei einer Firma zu antworten und bieten dabei noch weitere Unterstützung an. Dazu wählen sie Namen von Unternehmen, an die sich Millionen Menschen wenden, beispielsweise ein großer Softwareanbieter oder eine renommierte Bank. Wenn der Adressat das Produkt oder den Service nicht nutzt, wird er die E-Mail, den Anruf oder die Nachricht ignorieren. Im anderen Fall besteht aber eine gute Chance, dass er reagiert, weil er tatsächlich Hilfe wegen eines Problems braucht (beispielsweise ein Computerproblem).

Der Ansprechpartner, der in Wirklichkeit ein Betrüger ist, gibt vor, erst einmal „Ihre Identität prüfen“ zu müssen und bittet Sie, sich an „seinem System anzumelden“ oder sich bei Ihrem Rechner einzuloggen und ihm dann Fernzugriff auf Ihren Computer zu geben, damit er diesen für Sie „reparieren“ kann. Oder der Kriminelle gibt Ihnen die Befehle durch, damit Sie Ihren Rechner unter seiner Anleitung selbst reparieren können. Der Betrüger kann sich so später Zugang zu Ihrem Rechner verschaffen.

Beispiel 5: Misstrauen wecken

Einige Social-Engineering-Tricks zielen darauf, Misstrauen zu säen oder Streit zu verursachen. Oft sind dabei Menschen beteiligt, die der Benutzer kennt und böse auf ihn sind. Oder es handelt sich um Provokateure, die einfach nur Unruhe stiften möchten. Diese Menschen wollen zunächst Misstrauen bei dem Benutzer gegenüber anderen wecken, um sich selbst als verständnisvoll zu präsentieren und sein Vertrauen zu gewinnen. Manchmal handelt es sich um Erpresser, die Informationen manipulieren und ihrem Opfer dann mit Veröffentlichung drohen. Diese Art von Social Engineering beginnt oft damit, dass sich der Kriminelle Zugang zu einem E-Mail- oder anderem Kommunikations-Account beispielsweise bei einem Instant-Messaging-Service, sozialen Netzwerk oder Chat-Forum verschafft. Dies erreicht er durch Hacking, Social Engineering oder einfach durch Erraten besonders schwacher Passwörter.

Der Betrüger ändert dann sensible oder private Nachrichten (auch Bilder und Audio) mithilfe von einfachen Bearbeitungsmethoden und leitet diese dann an andere weiter, um so Streit, Misstrauen oder Peinlichkeiten zu provozieren. Unter Umständen lässt der Kriminelle das so aussehen, als wäre die Nachricht versehentlich verschickt worden, oder er gibt vor, den Adressaten darüber zu informieren, was „wirklich los ist“. Alternativ dazu nutzt er das geänderte Material unter Umständen, um Geld von der gehackten Person zu erpressen.

Es gibt in der Praxis Tausende Varianten von Social-Engineering-Tricks. Dem Einfallsreichtum der Betrüger sind hier keine Grenzen gesetzt. Der Angreifer wird die Informationen wahrscheinlich auch an andere verkaufen, damit diese ebenfalls das Opfer, seine Freunde, die Freunde seiner Freunde und so weiter attackieren können.[14]

Social Engineering bezeichnet ganz allgemein jede Handlung, die eine Person zu einer Aktion veranlasst, die in ihrem eigenen Interesse liegen kann oder nicht.[15] Es ist die „Kunst und die Wissenschaft“, bei der ein Mensch einen anderen Menschen so manipuliert, dass letzterer nach seinem Willen handelt. Bei einem Social-Engineering-Betrug zielen die Angreifer häufig auf das schwächste Glied in der Computer-Sicherheitskette. Es ist sogar möglich, dass ein nicht angeschlossener Rechner als Mittel für eine Social-Engineering-Attacke dient. Wenn der Betrüger einen arglosen Menschen dazu bringt, einen Computer anzuschließen und einzuschalten, dann könnte dieser „nicht angeschlossene“ Computer für eine Attacke missbraucht werden.[16]

Social Engineering ist die einfachste Variante, um sich unbefugten Zugang zu einem BMS zu verschaffen. Zum Schutz gegen derartige Angriffe müssen die Unternehmen ihre Mitarbeiter, externen Dienstleister und Geschäftspartner entsprechend schulen. Unter Umständen sind auch Sicherheitstrainings im Rahmen des On-Boarding-Prozesses von neuen Mitarbeitern oder externen Dienstleistern erforderlich.

Einige Unternehmen spielen mithilfe von Bedrohungsmodellen die verschiedenen Ereignisketten durch, die zu einer Sicherheitsverletzung führen könnten. Bei einem BMS werden im Zuge dieser Bedrohungsmodellierung potenzielle Zugangspunkte identifiziert und die Zugriffsrechte von externen Dienstleistern und Benutzern klar definiert (beispielsweise unter Verwendung des „Principle of Least Privilege“, bei dem Zugriffsrechte auf das jeweils erforderliche Minimum eingeschränkt werden). Richtlinien, Prozesse und Schulungen müssen dann entsprechend den Ergebnissen dieses Bedrohungsmodells entwickelt werden.

Insider-Angriffe, bei denen BMS-Systeme und -Prozesse sabotiert werden, können enormen Schaden verursachen. Schulungsprogramme sind ein wichtiges Instrument zum Schutz vor diesen Gefahren. Tabelle 3 zeigt die Kernelemente eines Programms für BMS-Sicherheitsschulungen:

Tabelle 3

Elemente zur Stärkung der BMS-Cybersicherheit

HR	Interne Aus- und Weiterbildung	Richtlinien und Prozesse
• Start bei Einstellungsprozess, Deaktivierung bei Kündigung	• Sonderschulungen für Manager und HR-Mitarbeiter	• Implementierung des Principle of Least Privilege, Aufgabentrennung, strenge Regeln für das Passwortmanagement, Änderungskontrollen
• Protokollierung und Überwachung von Aktivitäten	• Jährliche Auffrischungskurse zur Sensibilisierung	• Sicherung und Wiederherstellung
• Suchen und Antizipieren von Problemen, die zu böswilligen Handlungen führen können	• Schulung von externen Dienstleistern und Geschäftspartnern	• Sanktionen für Verstöße einführen und kommunizieren

[14]http://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering#close

[15]Social-Engineering.org

[16]http://www.textfiles.com/russian/cyberlib.narod.ru/lib/cin/se10.html

Fazit

Die Einführung von Sicherheitsrichtlinien zum Schutz der Netzwerkinfrastruktur für Gebäudemanagement-Systeme erfordert die Unterstützung durch die Unternehmensführung. Eine wirkungsvolle Defense-in-Depth und Defense-in-Breadth muss permanent gepflegt werden. Angriffe (darunter auch Social Engineering) werden immer zahlreicher und raffinierter. Deshalb müssen Prozesse und Verfahren zur Sicherung von BMS-Netzwerken entwickelt werden. Ein kritischer Erfolgsfaktor ist dabei die Schulung der Personen, die für den Betrieb der Gebäudemanagement-Systeme zuständig sind. Die umsichtige und sorgfältige Pflege von BMS-Netzwerken umfasst die konsequente Installation neuester Updates und die Weiterentwicklung von Strategien, die auf Defense-in-Depth- und Defense-in-Breadth-Sicherheitsarchitekturen basieren. Schulungen von Endanwendern/Mitarbeitern zum Schutz gegen Social-Engineering-Attacken sollten regelmäßig durchgeführt werden. Die Unternehmen profitieren von diesen Investitionen durch Reduzierung sicherheitsrelevanter Ereignisse, die Umsatzausfälle verursachen, und durch Wahrung ihrer Reputation bei Kunden und Partnern.

Über den Autor

Daniel Paillet ist Cyber Security Lead Architect im Geschäftsbereich Energy Management von Schneider Electric. Zuvor arbeitete er für das amerikanische Verteidigungsministerium an verschiedenen Sicherheitsprojekten. Er verfügt über mehr als 15 Jahre Erfahrung in der Entwicklung und Umsetzung von Sicherheitskonzepten in den Bereichen Informationstechnologie, Betriebstechnik, Retail, Banking und Point-of-Sale. Neben einer CISSP- und CEH-Zertifizierung besitzt er weitere anbieterunabhängige und anbieterspezifische Zertifizierungen. Aktuell ist er für die Gestaltung, Verbesserung und Entwicklung sicherer Lösungen und Angebote bei Schneider Electric zuständig.

Hinweis: Internet-Links können mit der Zeit veralten. Die angegebenen Links waren zu dem Zeitpunkt der Verfassung dieses White Paper gültig, können jetzt aber unter Umständen auf nicht mehr vorhandene Seiten verweisen.

Schneider Electric GmbH
Gothaer Str. 29, 40880 Ratingen / Germany

998-2095-12-08-15AR0_DE 11/19

Tel.: +49 (0) 2102 404 6000

www.se.com