heise Business Services

Ein eBook von

Powered by RAPID7

Cybersecurity für kritische Infrastrukturen

- **Wenn plötzlich das Licht ausgeht**
  Angriffe auf kritische Infrastrukturen
- **Cybersecurity: wie tägliches Zähneputzen**
  Aufbau eines effektiven Schutzes
- **Erste Hilfe gegen Hacker**
  Wie Security-Werkzeuge helfen können

Case Study
Energie Südbayern

Titelbild: maksheb, Bigstockphoto.com

Editorial

Cyber-Security ist ein Thema, das alle Unternehmen betrifft, ein gelungener Angriff kann empfindliche Folgen für die betroffene Firma haben. Von besonderem Interesse ist das Thema aber für die Betreiber so genannter Kritischer Infrastrukturen (KRITIS) – dazu gehören etwa Energie- oder Wasserversorger, aber auch Krankenhäuser. Passiert dort etwas, sind viele Menschen betroffen, die dann beispielsweise ohne Strom dastehen oder deren medizinische Versorgung gefährdet ist.

Lesen Sie im ersten Artikel dieses eBooks, wie das Bundesamt für Sicherheit in der Informationstechnik sich Sicherheitslage für die KRITIS-Betreiber einschätzt und was die Politik unternimmt, um möglichen Ausfällen entgegenzuwirken.

Im zweiten Artikel geht es darum, wie sich Unternehmen vor Angriffen schützen können – wichtiger Baustein hierbei sollte das Schwachstellenmanagement sein. Flankierend dazu sollten Werkzeuge wie Security Information and Event Management und Tools für Incident Detection and Response zum Einsatz kommen – mehr dazu lesen Sie im dritten Artikel.

Abschließend erfahren Sie im letzten Teil des eBooks, welche Maßnahmen Energie Südbayern ergriffen hat, um möglichen drohenden Ausfällen infolge von Cyber-Attacken entgegenzuwirken.

Ich wünsche Ihnen eine spannende Lektüre!

Martin Seiler
Associate Director, Heise Business Services

Heise Medien GmbH & Co.KG
Abt. Heise Business Services
Hans-Pinsel-Straße 10b
85540 Haar bei München

Registergericht:
Amtsgericht Hannover HRA 26709

Persönlich haftende Gesellschafterin:
Heise Medien Geschäftsführung GmbH

Registergericht:
Amtsgericht Hannover, HRB 60405

Geschäftsführer:
Ansgar Heise, Dr. Alfons Schräder

Verantwortlich für den Inhalt:
Heise Business Services
Thomas Jannot, tj@heise.de

Haben Sie Fragen zu diesem eBook oder haben Sie Interesse an einer eigenen Produktion, dann schicken Sie bitte eine E-Mail mit dem Betreff **„HBS-eBook“** an hbs@heise.de

Inhalt

Wenn plötzlich das Licht ausgeht **4**
Angriffe nehmen zu 4
Einheitliche Richtlinien 6
Unternehmen müssen aktiv werden 6

Cybersecurity: wie tägliches Zähneputzen **9**
Fünf Grundsätze der Cybersecurity 9
Schützen, Erkennen, Bekämpfen 10
Schwachstellenmanagement schließt Lücken 10
Auswahlkriterien fürs richtige Tool 12
Keine hundertprozentige Sicherheit 12

Erste Hilfe gegen Hacker **14**
206 Tage unentdeckt 14
Schutz automatisieren 16
Was tun im Fall der Fälle? 17

Case Study: Energie Südbayern **18**

ÜBER DEN AUTOR

Bernd Müller ist Journalist für Technologie und Wissenschaft. Er war Redakteur bei Bild der Wissenschaft und der Wirtschaftswoche sowie PR-Referent bei der Fraunhofer-Gesellschaft. Seit vielen Jahren schreibt er für Verlage und Unternehmen zu Innovationsthemen, außerdem forscht und lehrt er zum Thema Wissenschaftskommunikation.

Wenn plötzlich das Licht ausgeht

> Hacker-Angriffe auf Kritische Infrastrukturen nehmen zu.

> Deutschland steht mehr denn je im Fokus von Cyber-Angrffen.

Angriffe auf Kritische Infrastrukturen häufen sich. Studien zeigen: Die Betreiber sind darauf nicht ausreichend vorbereitet. Ein Lagebericht.

Wer den Schaden hat, braucht für den Spott nicht zu sorgen. Als kurz vor dem Jahresende 2019 bekannt wurde, dass Citrix eine schwere Sicherheitslücke aufweist, war der Name für den Hack schnell gefunden: Shitrix. Der Fernzugriffsdienst, der die Wartung von IT-Systemen erleichtern soll, erleichterte offenbar auch das Eindringen von Hackern. Die können beliebigen Schadcode auf den IT-Systemen ihrer Opfer ausführen. Schon kurz nach dem Bekanntwerden der Lücke kursierten im Internet Anleitungen zum Angriff und es wurden auch erste Attacken gemeldet. Unter den betroffenen Unternehmen waren etliche Betreiber Kritischer Infrastrukturen (KRITIS).

Angriffe nehmen zu

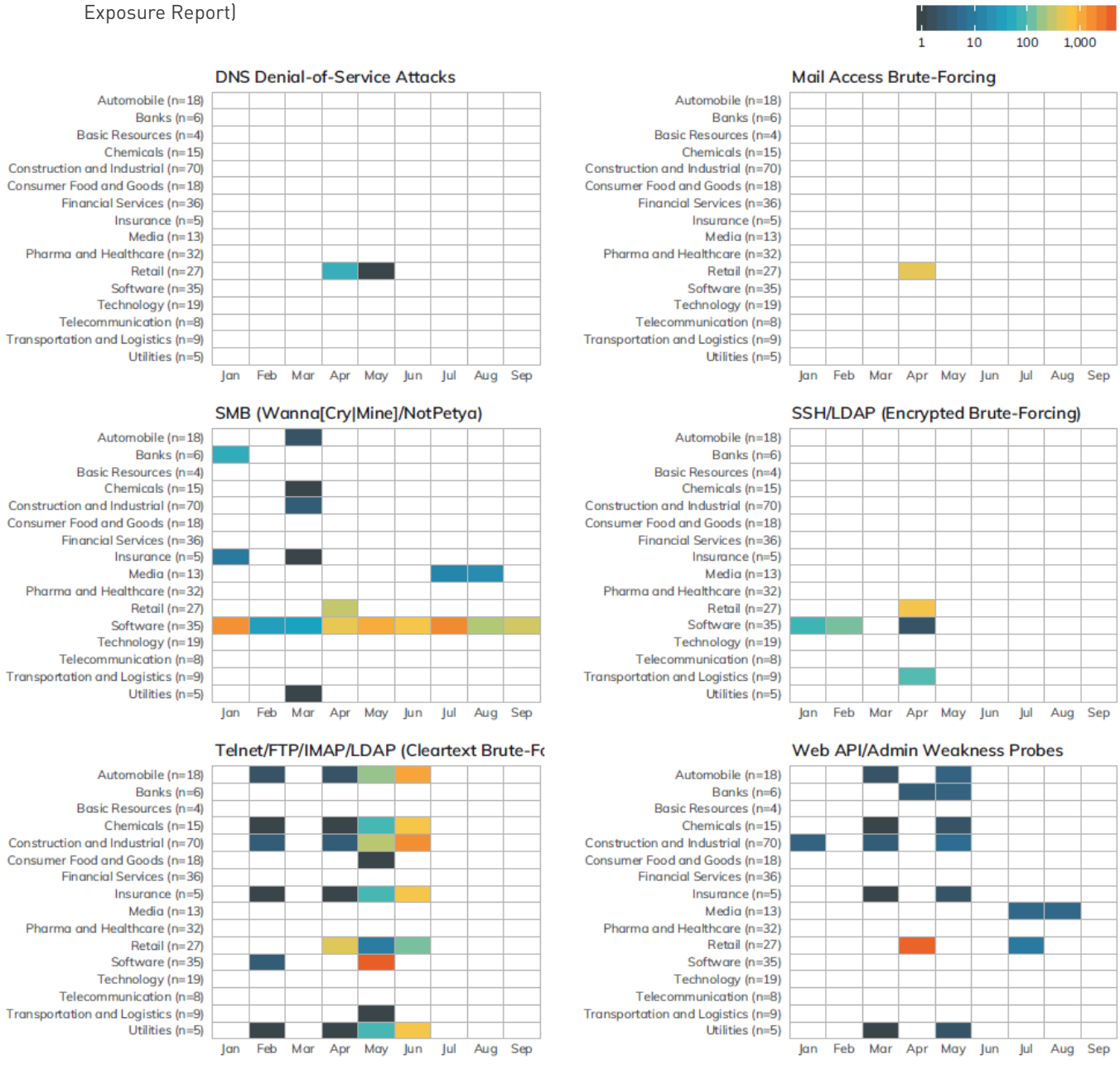
Das BSI hat in der letzten Zeit eine deutliche Zunahme von Hacker-Angriffen auf Kritische Infrastrukturen registriert. In der zweiten Jahreshälfte 2018 habe das BSI von 157 solchen Attacken erfahren, davon 19 auf das Stromnetz. Aber nicht jede Meldung sei ein Angriff, beschwichtigt das BSI, auch technische Fehler würden gemeldet und in diese Zahl eingehen. BSI-Präsident Arne Schönbohm warnt dennoch: „Diese Angriffe zeigen, dass Deutschland mehr denn je im Fokus von Cyber-Angriffen steht. Dass bislang keine kritischen Netzwerke infiltriert werden konnten, zeigt, dass das IT-Sicherheitsniveau der deutschen KRITIS-Betreiber auf einem guten Level ist."

Aber möglicherweise nicht gut genug. Denn immer wieder werden Vorfälle bekannt. So kostete 2016 ein Angriff mit Ransomware das Lukaskrankenhaus in Neuss rund eine Million Euro. Am 27. Juni 2017 meldete Maersk, die größte Containerschiffreederei der Welt, dass aufgrund einer Cyberattacke IT-Systeme über mehrere Geschäftsteile hinweg ausgefallen seien. Die Angreifer setzten offenbar die berüchtigte Erpressungssoftware NotPetya ein, die Computer der Opfer verschlüsselt und erst gegen Zahlung eines Lösegelds wieder freigibt. Von der Attacke waren auch deutsche Unternehmen betroffen – wie schon sechs Wochen zuvor bei den Computerausfällen durch den Verschlüsselungstrojaner

Zeichen für bösartige Aktivitäten nach Branche

Je nach Branche schwanken die beobachteten bösartigen Aktivitäten. (Quelle: Rapid7, Industry Cyber-Exposure Report)

WannaCry, wodurch unter anderem die Zugdurchsagen der Deutschen Bahn ausfielen. Schwacher Trost für Maersk: Die Attacke war nicht gezielt gegen die Reederei gerichtet, der Ausfall war ein Kollateralschaden eines Angriffs, mit dem Hacker auf gut Glück ins Blaue schossen. Bei solchen „Schrotschüssen" treffen Angreifer auch immer wieder Kritische Infrastrukturen.



KRITIS-Definition

Kritische Infrastrukturen (KRITIS) sind laut BSI „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden." Die gibt es vor allem in den Branchen Energie, Informationstechnik, Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen, Staat und Verwaltung sowie Medien und Kultur.

Deutsche Unternehmen mit Sicherheitslücken

Wie steht es um die Verwundbarkeit und Resilienz deutscher Unternehmen gegenüber Bedrohungen aus dem Internet? Diese Frage beantwortet der fünfte Industry Cyber Exposure Report, den Rapid7 im Oktober 2019 vorgestellt hat. Die Untersuchung umfasst die 320 Unternehmen des Deutsche Börse Prime Standard. Untersucht wurden

- **Die Zahl der sichtbaren Server und Geräte**
- **Die Zahl gefährdeter und unsicherer Geräte**
- **Der Status zur Abwehr von Phishing**
- **Schlechte Konfiguration von öffentlichen Services und Metadaten**
- **Risiken in Verbindung mit Webseiten Dritter**

Einheitliche Richtlinien

Auch die Politik hat das Thema auf dem Schirm. 2016 trat die Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS) in Kraft, die 2018 in nationales Recht umgesetzt werden musste. Die NIS-Richtlinie ist die erste EU-weite Rechtsvorschrift über Cybersicherheit und soll besonders auch kritische Infrastrukturen schützen. Mit der Richtlinie wurde ein einheitlicher Rechtsrahmen für den EU-weiten Aufbau nationaler Kapazitäten für die Cyber-Sicherheit geschaffen. Vereinbart wurde zudem eine stärkere Zusammenarbeit der Mitgliedstaaten der Europäischen Union sowie Mindestsicherheitsanforderungen an und Meldepflichten für Kritische Infrastrukturen sowie für bestimmte Anbieter digitaler Dienste wie Cloud-Services und Online-Marktplätze.

„Bisher hatten wir in Deutschland noch keinen Großschadensfall, der aus einem Cybervorfall entstanden ist", sagt Johannes Rundfeldt in einem aktuellen Interview mit dem Spiegel. Für den Leiter der Arbeitsgemeinschaft Kritische Infrastrukturen (AG KRITIS), sind erfolgreiche Angriffe aber keine Frage mehr des „ob", sondern nur noch des „wann". Die AG KRITIS plane, ein Cyber-Hilfswerk aufzubauen nach dem Vorbild des Technischen Hilfswerks THW.

Unternehmen müssen aktiv werden

Und die Bundesregierung? Sie tut, was Regierungen in solchen Fällen immer tun: Sie richtet eine neue Behörde ein. Die Agentur für Cybersicherheit, die in der Region Halle-Leipzig angesiedelt wird, soll Forschungs- und Entwicklungsvorhaben mit hohem Innovationspotenzial für die IT-Sicherheit fördern und finanzieren. Solche staatlichen Maßnahmen sind wichtig, halten aber Hacker nicht ab. Dazu müssen die Betreiber der Kritischen Infrastrukturen selbst aktiv werden.

Hier ein kurzer Auszug aus den Ergebnissen:

- **DB 320 Organisationen haben im Durchschnitt eine öffentliche Angriffsfläche von 88 Servern/Geräten, viele Unternehmen auch über 300 Systeme/Geräte.**
- **295 der Unternehmen (91%) haben schwache oder nicht vorhandene Anti-Phishing-Abwehrmaßnahmen. Dies ist der schlechteste Wert aller bisherigen Reports.**
- **Die Mehrheit (94%) der Unternehmenswebsites haben eine SSL/TLS-Verschlüsselung, während 21 (6%) der DB 320-Organisationen dies nicht haben. Sie lassen ihre Webseiten offen für Angreifer, die Webinhalte verändern können.**
- **Elf der 19 Industriesektoren hatten mindestens eine Organisation mit Malware-Infektion. Die Vorfälle in den verschiedenen Branchen reichen von Missbrauch für Denial-of-Service (DoS)-Attacken bis hin zu Angriffen, die WannaCry und NotPetya ähneln.**
- **Die meisten Unternehmen bieten auf ihren Webseiten Dienste an, die auf stark veralteter Software basieren.**

Der Report weist einige ernstzunehmende Sicherheitslücken nach und fragt: Wenn schon die DB 320 Organisationen, die in der Regel über beträchtliche Ressourcen und Zugang zu guter technischer Expertise verfügen, so schwach abschneiden, wie mag es dann um die Sicherheit vieler kleinerer Unternehmen und öffentliche Einrichtungen bestellt sein?

Doch daran hapert es, wie der Industry Cyber Exposure Report von Rapid7 belegt (siehe Kasten auf dieser und der vorigen Seite). Manche Schwachstellen seien seit Jahren bekannt und würden dennoch nicht behoben. Auch nach dem eingangs erwähnten Citrix-Vorfall versäumten es hunderte Kunden in Deutschland, den provisorischen Sicherheitspatch aufzuspielen, obwohl die AG KRITIS und das BSI darüber informiert hatten. Entweder scheinen die Organisationen und ihre IT-Dienstleister mit der Aktualisierung überfordert zu sein, die Dringlichkeit nicht verstanden zu haben oder die Informationen nicht die richtigen Adressaten gefunden zu haben, mutmaßt die AG KRITIS.

Was sollten die Betreiber kritischer Infrastrukturen tun? Zunächst müssen sie ihre Hausaufgaben machen. Dazu gehört, dass sie für alle drei Säulen der Cybersicherheit – Protection, Detection, Defense – ihre Fähigkeiten stärken. Zur ersten Säule, dem vorbeugenden Schutz, gehört ein Schwachstellen-Management, das Sicherheitslücken erkennt und schließt, bevor Hacker sie ausnutzen können (siehe Seite 9). Wenn ein Angriff dagegen schon passiert ist, muss er erstens schnellstmöglich entdeckt und zweitens schnellstmöglich unterbunden werden. Traditionell werden dazu SIEM-Systeme eingesetzt, die allerdings nur beim Entdecken des Angriffs helfen. Welche modernen Möglichkeiten es gibt, um beides zu bewältigen, erläutert der Beitrag auf Seite 14.

	Pflicht zur Umsetzung IT-Sicherheit nach Stand der Technik	Pflicht zur Überprüfung der Absicherung (z.B. durch Audit)	Unverzügliche Versorgung mit relevanten Informationen durch BSI	Meldepflicht von IT-Sicherheitsvorfällen	Möglichkeit der Beratung und Unterstützung durch das BSI
KRITIS-Betreiber gemäß BSI-KRITIS-Verordnung (bis auf die nachfolgend aufgelisteten Sonderfälle)	Ja. Konkretisierung in Branchen spätestens 2 Jahre nach Inkrafttreten der Verordnung.	Ja. Überprüfung und Nachweis alle 2 Jahre, erstmalig 2 Jahre nach Inkrafttreten der Verordnung.	Ja.	Ja. Spätestens 0,5 Jahre nach Inkrafttreten der Verordnung.	Ja.
Öffentliche Telekommunikationsnetze gemäß BSI-KRITIS-Verordnung	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §109 TKG. (Altere-gelung)	BNetzA überprüft Umsetzung alle 2 Jahre.	Ja.	Ja, sofort. Meldepflicht an die BNetzA (Erweiterung einer Altregelung)	Ja.
Öffentliche Telekommunikationsnetze (sonstige Betreiber)	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §109 TKG. (Altere-gelung)	BNetzA überprüft Umsetzung alle 2 Jahre.	Nein.	Ja, sofort. Meldepflicht an die BNetzA (Erweiterung einer Altregelung)	Nein.
Energieversorgungsnetze gemäß BSI-KRITIS-Verordnung	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1a) EnWG (Erweiterung einer Altregelung)	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1a) EnWG	Ja.	Ja. Mit Inkrafttreten der Verordnung.	Ja.
Energieversorgungsnetze (sonstige Betreiber)	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1a) EnWG (Erweiterung einer Altregelung)	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1a) EnWG	Nein.	Nein.	Nein.
Energieanlagen gemäß BSI-KRITIS-Verordnung	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1b) EnWG	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1b) EnWG	Ja.	Ja. Mit Inkrafttreten der Verordnung.	Ja.
Genehmigungsinhaber nach § 6, 7 oder 9 Atomgesetz (z.B. Kernkraftwerke, atomare Lager)	Ja. (Keine Änderung zum bestehenden Atomgesetz)	Ja. (Keine Änderung zum bestehenden Atomgesetz)	Ja.	Ja. (seit 25.07.2015)	Nein. Es sei denn, Sie sind KRITIS-Betreiber.

Übersicht zu den Neuregelungen für KRITIS-Betreiber

Mit dem IT-Sicherheitsgesetz werden für KRITIS-Betreiber im Wesentlichen fünf Neuerungen eingeführt. (Quelle: BSI, Bundesamt für Sicherheit in der Informationstechnik)

Cybersecurity: wie tägliches Zähneputzen

Beim Aufbau eines effektiven Schutzes gegen Cyberangriffe gilt es einige Grundsätze zu beachten. Ein wirksamer Schutz gegen Hacker ist das Schwachstellenmanagement.

Wenn es um die Cybersicherheit geht, bekommen Sicherheitsexperten von ihrem Management häufig dies zu hören: „Erstmal ist das Geschäft wichtig, um die Sicherheit kümmern wir uns später." Diese Haltung ist brandgefährlich und am Ende meist teurer. Security lässt sich nämlich nachträglich nur schwer über einen bestehenden Prozess stülpen. Besser als Löcher zu stopfen ist es, erst gar keine Löcher entstehen zu lassen. Security muss deshalb schon am Anfang jeder Projektplanung mitgedacht und auch im Budget verankert werden.

> Security muss schon am Anfang mitgedacht werden.

Fünf Grundsätze der Cybersecurity

Wie das geht, hat das Center für Internetsicherheit (CIS) in seinem CIS Controls Report zusammengetragen. Die gemeinnützige Organisation identifiziert, entwickelt, validiert und fördert Best Practices in der Cybersecurity. Laut CIS basiert ein effektiver Schutz auf fünf Grundsätzen:

- **Lernen:** Eine effektive Abwehr kann man am besten entwickeln, wenn man aus aktuellen Angriffen lernt, und zwar kontinuierlich. Um sich nicht zu verzetteln, sollte man nur solche Maßnahmen ergreifen, die schon bewiesen haben, dass sie reale Angriffe abwehren können.
- **Priorisieren:** Als erstes sollte man in Maßnahmen investieren, die vor den größten Bedrohungen schützen und die mit überschaubarem Aufwand umgesetzt werden können. Davon ausgehend können sich Unternehmen dann speziellere Bedrohungen vornehmen.
- **Messen:** Kennzahlen und Metriken helfen, eine gemeinsame Sprache für Führungskräfte, IT-Spezialisten, Auditoren und Sicherheitspersonal zu etablieren. So lassen sich erforderliche Anpassungen schneller identifizieren und umsetzen.

- **Prüfen:** Eine regelmäßige Validierung der Wirksamkeit der aktuellen Sicherheitsmaßnahmen erleichtert die Priorisierung der nächsten Schritte.
- **Automatisieren:** Werkzeuge helfen, das aktuelle Sicherheitsniveau im Blick zu behalten und kontinuierlich Änderungen vorzunehmen.

Schützen, Erkennen, Bekämpfen

Auf Basis dieser Grundsätze empfiehlt CIS 20 grundlegende Maßnahmen für die Sicherheit. Dazu gehören eine Bestandsaufnahme von Hardware und Software, das Verwalten von Zugriffsrechten, Datensicherung und einige weitere. Sie lassen sich grob drei Etappen zuordnen: Protection, Detection und Defense. Der erste Punkt, das Vorbeugen, ist mit am Wichtigsten. Ist der Schutz so gut, dass Hacker unverhältnismäßig viel Aufwand investieren müssen, um in ein IT-System einzudringen, verlieren sie meist schnell das Interesse – wie ein Einbrecher, der nach zwei Minuten das Fenster immer noch nicht aufgehebelt hat. Viele Angriffe erfolgen auch gar nicht gezielt, sondern gleichen Schrotschüssen, bei denen immer irgendein Ziel getroffen wird. Damit das in der eigenen Organisation nicht passiert, müssen Lücken laufend identifiziert und geschlossen werden. Die Grundlage dafür ist ein Schwachstellenmanagement, auf das dieser Beitrag näher eingeht. Weitere Maßnahmen fokussieren auf das Erkennen und Bekämpfen von bereits erfolgten Angriffen. Hier kommt das Security Information and Event Management ins Spiel mit einem Incident Response Management. Beides beleuchtet der Beitrag auf Seite 9 näher.

> Sicherheitslücken müssen laufend identifiziert und geschlossen werden.

Schwachstellenmanagement schließt Lücken

Hier soll es um das Schwachstellenmanagement gehen, für das es etliche Werkzeuge gibt. Sie erkennen, melden und beheben Sicherheitsschwachstellen in Geschäftsprozessen, Webanwendungen und Betriebssystemen sowie in der darauf ausgeführten Software. Das geschieht kontinuierlich, denn nur so lassen sich neue Schwachstellen frühzeitig – nach Stunden, besser noch nach Minuten – erkennen, wenn sich in Netzwerken, Systemen und Anwendungen etwas ändert. Man kann das Schwachstellenmanagement vergleichen mit dem täglichen Zähneputzen – es verhindert, dass sich kleine Probleme anhäufen, die irgendwann zu einer großen (Zahn)Lücke führen. Doch auch mit der besten Zahnpflege ist es ratsam, mindestens einmal im Jahr zum Zahnarzt zu gehen. Der findet vielleicht Karies an Stellen, wo die Zahnbürste nicht hinkommt. Auf die Cybersi-

> Neue Schwachstellen möglichst frühzeitig erkennen.

cherheit übertragen entspricht der Zahnarztbesuch einem Penetration-Test, bei dem Experten mit Hackermethoden im Auftrag des Kunden versuchen, Lücken im Schutzwall zu finden. Bei Schwachstellenmanagement, Penetration-Tests und anderen vorbeugenden Maßnahmen wie regelmäßigen Updates oder Schulungen der Mitarbeiter gibt es kein Entweder-oder – alles ist wichtig, aber ohne Schwachstellenmanagement geht es nicht.

Grundlegende Maßnahmen für mehr Sicherheit

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Das CIS empfiehlt 20 Bausteine, mit denen Sie für mehr Sicherheit sorgen können. (Quelle: Center für Internetsicherheit, CIS)

> Ohne Schwachstellenmanagement geht es nicht.

Ein Hacker muss nur einmal etwas richtig machen.

Auswahlkriterien fürs richtige Tool

Unternehmen und Betreiber Kritischer Infrastrukturen haben angesichts des großen Angebots an Tools die Qual der Wahl. Kriterien zur Auswahl sind unter anderen die vollständige Erfassung von Assets und Abdeckung bei Scans, eine effiziente Priorisierung der Schwachstellen nach Kritikalität sowie die Unterstützung beim Remediations-Prozess. Darüber hinaus gibt es Dutzende weitere Eigenschaften, die ein gutes Tool mitbringen sollte. Sie lassen sich einteilen in

- → **grundlegende Eigenschaften (wie Implementierung und Skalierbarkeit)**
- → **Schwachstellenanalyse im Netzwerk**
- → **Priorisierung**
- → **Beheben von Schwachstellen**
- → **Reporting**
- → **Compliance- und Konfigurationsanalyse**
- → **Administration**
- → **Integration**
- → **Eigenschaften des Anbieters**

Welche Aspekte jeweils wichtig sind und welche Fragen Sie einem Anbieter stellen sollten, erläutert der Kundenratgeber Schwachstellen-Management-Lösungen von Rapid7 (https://www.rapid7.com/de/info/auswahl-der-schwachstellen-management-loesung/).

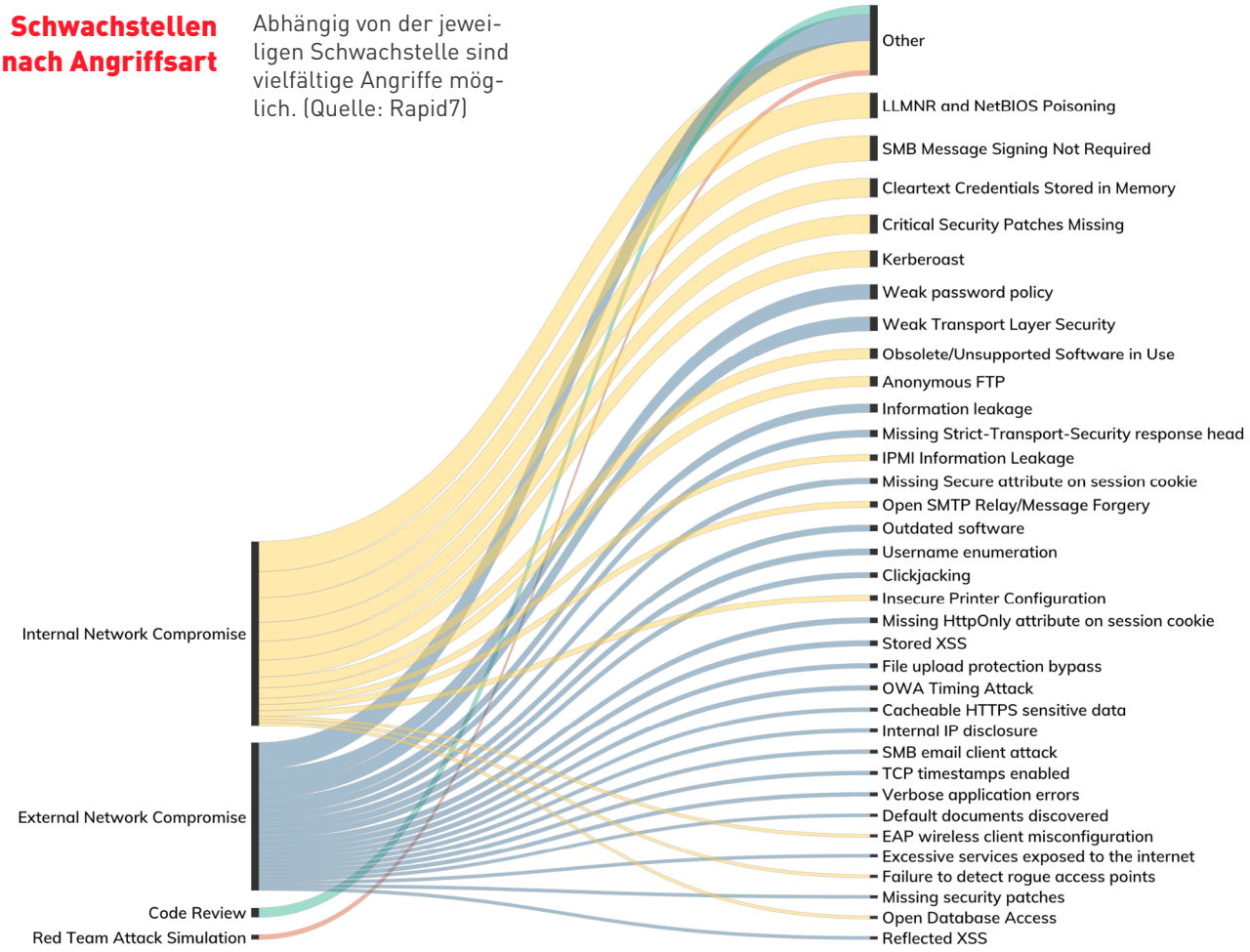
Keine hundertprozentige Sicherheit

Angenommen, ein Unternehmen hat mit Hilfe dieses Ratgebers ein gutes Werkzeug gefunden und setzt alle Maßnahmen vorbildlich um – ist es dann ein für alle Mal gegen Hacker gefeit? Leider nein, denn endgültige Sicherheit wird es niemals geben. Ursache ist ein Ungleichgewicht der Kräfte. Ein Unternehmen und alle seine Mitarbeiter müssen stets alles richtig machen, um sich umfassend zu schützen. Ein Hacker dagegen muss nur einmal etwas richtig machen, vielleicht auch nur Glück haben, um an brisante Informationen zu gelangen oder Anlagen lahmzulegen. Sicherheit ist deshalb kein Zustand, sondern ein fortwährender Prozess. Alles, was heute gebaut und als vermeintlich sicher eingestuft wird, wird in ein paar Jahren angegriffen. Das gilt zum Beispiel für Verschlüsselungstechniken, die schon in wenigen Jahren von immer schnelleren Computern gebrochen werden, erst recht, wenn Quantencomputer serienreif werden. Sicherheit sollte daher ein integraler Bestandteil aller Produkte und Dienstleistungen schon in der Entwicklungsphase sein.

So wichtig Prävention ist, Unternehmen sollten sich auch darauf vorbereiten, Angriffe zu erkennen und abzuwehren – dann sind Detektion und Reaktion gefragt. Manche Angriffe dauern Wochen und mit geeigneten Mitteln und Spezialisten an Bord lässt sich der Schaden abwenden und gleichzeitig noch etwas für die künftige Sicherheit lernen. Wie das geht, erläutert der Beitrag Erste Hilfe gegen Hacker auf Seite 14.

Schwachstellen nach Angriffsart

Abhängig von der jeweiligen Schwachstelle sind vielfältige Angriffe möglich. (Quelle: Rapid7)



Erste Hilfe gegen Hacker

Unternehmen werden unablässig von Hackern attackiert – und merken es oft gar nicht oder reagieren viel zu spät. Helfen können Werkzeuge wie Security Information and Event Management und Tools für Incident Detection and Response.

Wenn Sie hören, dass Einbrecher in der Gegend unterwegs sind – was würden Sie tun? Die Haustüre offenlassen, wenn Sie das Haus verlassen, und Geld und Schmuck auf den Küchentisch legen, damit die Einbrecher nicht lange suchen müssen? Klingt idiotisch, ist aber so ähnlich wie das, was manche Unternehmen machen. Sie wissen, dass die Tore ihrer IT sperrangelweit offenstehen, und trotzdem unternehmen sie nichts dagegen. Hacker haben dann leichtes Spiel. Im Internet kursieren Anleitungen, wie Hacker Sicherheitslücken spielend leicht ausnutzen können. Das Ärgerliche dabei ist, dass diese Lücken zum Teil lange bekannt sind. Manche Wochen, manche aber schon Monate oder gar Jahre. Die Unternehmensjuwelen – Baupläne, Kostenkalkulationen, Softwarecode – liegen dann im übertragenen Sinne auf dem Küchentisch.

„

Im Schnitt dauert es 206 Tage, bis ein Angriff entdeckt wird.

„

Viele Lücken sind zum Teil lange bekannt.

206 Tage unentdeckt

Was die Sache noch schlimmer macht: Viele Unternehmen merken den Diebstahl selbst dann noch nicht, wenn der Dieb bereits auf der Flucht ist. Eine aktuelle Studie des Ponemon Instituts hat herausgefunden, dass es im Schnitt 206 Tage dauert, bis ein Angriff entdeckt wird und noch einmal 73 Tage, um die Schäden zu beheben. Verblüfft waren auch die Experten von Rapid7 bei den Recherchen für ihren Industry Cyber Exposure Report. Selbst im Zeitraum der Untersuchungen stellten sie Kompromittierungen fest, auf die offenbar niemand reagierte.

Woran liegt es, dass die Unternehmen mit ihren Sicherheitsmaßnahmen so weit hinterherhinken? Ein Grund ist, dass der IT-Fußabdruck – die Gesamtheit aller IT-Assets im Unternehmen – ständig größer wird. In den letzten Jahren etwa durch die Bring-your-Own-Device-Politik, die das Einbinden von privaten Smartphones in die Unternehmens-IT vorsieht. Ein durchschnittliches Unternehmen überwacht Hunderte von Anwendungen, mehrere Clouds, firmeninterne Anlagen und Endpunkte auf mehreren Kontinenten.

Bessere Compliance bei 60 Prozent Zeitersparnis

„Irgendwas ist anders als sonst." Solche Nachrichten hat Benjamin Nawrath, Information Security Officer bei Energie Südbayern, früher häufiger von Kollegen bekommen. Vielleicht ein Hacker-Angriff auf die Anlagen des Energieversorgers? Dann ging die Sucherei in den Logs los, was eine Menge Zeit kostete. Das ist vorbei, denn seit einiger Zeit betreibt das Unternehmen die Schwachstellenmanagement-Lösung InsightVM sowie InsightIDR, eine Lösung für Incident Detection and Response, beide von Rapid7. „InsightIDR hat mir dabei geholfen, schneller auf Vorfälle zu reagieren. Es ist sehr einfach zu nutzen und die Agents bieten einen großartigen Einblick", lobt Nawrath. Außerdem erleichtere es die Compliance mit dem deutschen IT-Sicherheitsgesetz.

InsightIDR vereinigt Security Information and Event Management (SIEM), User Behavior Analytics (UBA) und Endpoint Detection and Response (EDR), bedient wird es mit einem übersichtlichen Dashboard. Zusammen mit InsightVM spart Benjamin Nawrath 60 Prozent seiner Zeit. Das gebe ihm mehr Zeit für die Verifizierung der Schwachstellen. „Dank der Rapid7-Produkte bin ich in der Lage, das Top-Management von der tatsächlichen Risikosituation zu überzeugen. Ich erhalte dafür mehr Respekt für meine Arbeit", so Nawrath. „Und da die Lösungen nicht so teuer waren, war es kein Problem, das notwendige Budget zu bekommen."

Hier kommt traditionell das Security Information and Event Management (SIEM) ins Spiel. Es soll helfen, bereits erfolgte Angriffe schnell zu erkennen und zu bewältigen. Ein SIEM-System sammelt laufend die Sicherheitsdaten, die in der IT-Landschaft des Unternehmens anfallen und erzeugt Meldungen für verdächtige Aktivitäten.

Klingt gut, ist es aber häufig nicht. Während sich SIEM in der Finanzbranche und bei großen Unternehmen etabliert hat, fürchten kleine und mittelständische Unternehmen die Komplexität so einer Lösung. Damit liegen sie nicht ganz falsch. Denn es bedarf eines großen Aufwands, um zu definieren, was für ein Netzwerk „normal" und was „verdächtig" ist. Auch im täglichen Betrieb bleibt die Verwaltung komplex und bindet Ressourcen. Fast zwangsläufig kommt es zu einer Flut an Warnungen. Sicherheitsexperten ertrinken dann geradezu in unüberschaubaren – oft falsch positiven – Alarmen. Das schafft mehr Arbeit für die Teams und macht es schwierig, sich auf das wirklich Wichtige zu konzentrieren. Diese Überlastung führt zu einem traurigen Befund des Ponemon Instituts: Danach denken zwei Drittel des Sicherheitspersonals daran, ihren Job zu quittieren.

Schutz automatisieren

Weil die IT-Landschaften immer noch weiterwachsen, die Hackerangriffe nicht weniger werden und die Budgets vor allem in mittelständischen Unternehmen knapp bleiben, kann der Ausweg nur sein: SIEM-Systeme müssen intelligenter, und die Abwehrmaßnahmen effizienter und automatisierter werden. Wie das geht, erläutert der SIEM-Kundenratgeber von Rapid7 (https://www.rapid7.com/de/info/siem-buyers-guide/). Vor allem müssen SIEM-Lösungen drei wichtige Fähigkeiten haben:

- **Datensammlung:** Die Lösung muss Daten in ihrer Umgebung erheben und zentralisieren und das einfache Durchsuchen dieser Daten ermöglichen (mehr dazu auf Seite 8 des Ratgebers);
- **Analyse:** Die SIEM-Lösung muss Risiken und Bedrohungen identifizieren durch die Auswertung der Daten mithilfe verschiedener Techniken. Dazu reicht es nicht, nur Wenn-Dann-Regeln zu befolgen, sondern fortgeschrittene Methoden zu verwenden wie Honeypots, User Behaviour Analytics und vorgefertigte Erkennungsverfahren (mehr dazu auf Seite 9 des Ratgebers);
- **Gegenmaßnahmen:** Die Lösung muss dabei unterstützen, zu den Analyseergebnissen passende Maßnahmen mittels Orchestrierung und Berichterstattung zu ergreifen (mehr dazu auf Seite 10 des Ratgebers).

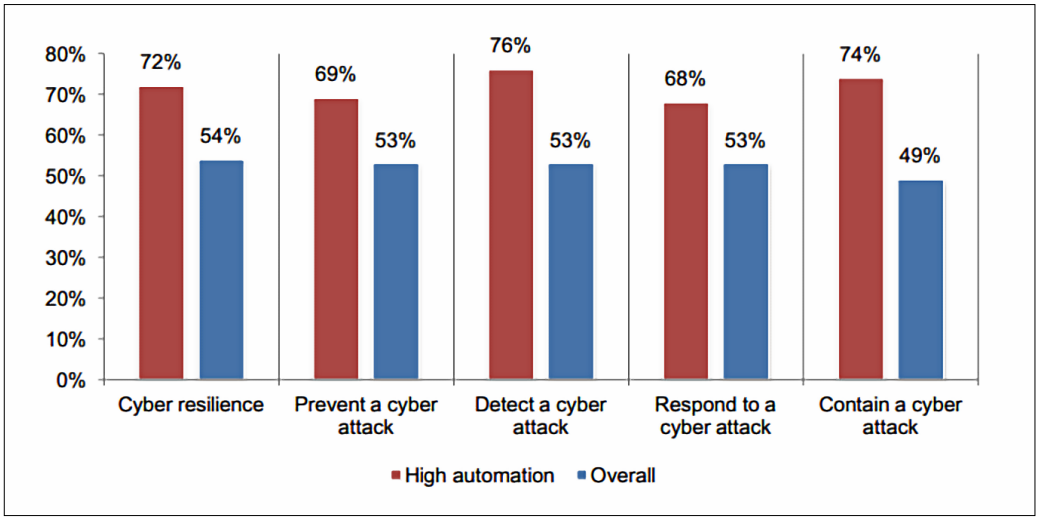
Wobei SIEM Sie unterstützt

Die drei meist verbreiteten Angriffsvektoren und wie SIEM helfen kann. (Quelle: Rapid7)

ANGRIFFSVEKTOR	WARUM TRANSPARENZ NOTWENDIG IST	WELCHE UNTERSTÜTZUNG SIEM BIETET
Schwachstellen	In mehr als 250 Szenarien haben Penetrationstester in 84 % der Fälle mindestens eine Schwachstelle in Produktionssystemen ausgenutzt.	Erkennt Aktivitäten (z. B. Rechteausweitungen und Lateral Movement), die im Zusammenhang mit der Ausnutzung von Schwachstellen auftreten.
Fehlkonfigurationen	In 80 % der Fälle wurde bei Penetrationstests mindestens eine Netzwerk-Fehlkonfiguration erfolgreich ausgenutzt. Bei Betrachtung aus der Innenperspektive steigt dieser Wert sogar auf 96 %.	Zeigt Fehlkonfigurationen von Benutzerkonten und Komponenten auf (z. B. unbekannte Administratoren, gemeinsam genutzte Konten und Überwachung der Dateiintegrität).
Zugangsdaten	Bei 53 % der Penetrationstests konnten mindestens einmal erfolgreich Zugangsdaten abgefangen werden.	Identifiziert verdächtige Authentifizierungen und löst ggf. Untersuchungs-Workflows aus.

Wer sich vornimmt, ein SIEM-System einzuführen, muss bei der Auswahl kritische Fragen stellen. Zuerst an sich selbst: Welche Ziele verfolgen wir mit der Implementierung einer SIEM-Lösung? Haben unsere Mitarbeiter die erforderlichen Kompetenzen, um ein klassisches regelbasiertes SIEM-System zu betreiben? Haben Sie eine Evaluation von Lösungen vorgenommen? Was für Daten werden erfasst? Wann muss ein Anwender tätig werden? Wie unterstützt uns das System bei Untersuchungen von Alerts und beim Ergreifen von Abwehrmaßnahmen? Diese und andere Fragen sind im SIEM-Kundenratgeber von Rapid7 zusammenfasst (https://www.rapid7.com/de/info/siem-buyers-guide/).

Automatisierung verbessert sowohl die Ausfallsicherheit als auch die Möglichkeiten, Cyberangriffe zu erkennen, zu verhindern und einzudämmen.



Von 1 = niedrig bis 10 = hoch (Quelle: Ponemon Report „The Cyberresilient company 2019)

Was tun im Fall der Fälle?

Was passiert, wenn es passiert ist – wenn ein schwerwiegender Angriff stattgefunden hat? Dann regiert das Chaos. IT-Systeme werden panisch heruntergefahren, wichtige Personen nicht informiert, vielleicht sogar Lösegeld an die Erpresser gezahlt. Alles falsch, denn im Fall des Falles gilt es, kühlen Kopf zu bewahren und die Schritte einzuhalten, die im Incident Response Plan stehen. Sofern man einen hat. Warum so ein Plan wichtig ist und wie man ihn entwickelt und aktuell hält, steht im Whitepaper „Vorbereitung für den Angriff: Entwicklung eines Incident Response Plan“ (https://information.rapid7.com/incident-response-planning-ebook-registration.html) des Sicherheitsdienstleisters Rapid7.

ANWENDERBERICHT

Rapid7 InsightVM und InsightIDR ermöglichen 60% Zeitersparnis und erleichtern die Compliance bei Energie Südbayern

Energie Suedbayern	Herausforderung	Ergebnis
Branche: Energieversorger	Die Compliance mit deutschem IT-Sicherheitsgesetz musste gewahrt bleiben.	Da ESB nachweisen konnte, dass die Technologie zum Zweck der Sicherheit eingesetzt wird, stimmte der Betriebsrat zu.
Größe: 420 Mitarbeiter	Intelligente Lösung zur Erkennung von anomalen Aktivitäten in der IT-Umgebung, die über einfache Regeln hinausgeht.	Rapid7 InsightVM und InsightIDR bieten vereinfachte Verwaltung und zentrale Berichte mit einem einzigen Agent.
Produkte: InsightVM*, InsightIDR		

Der Energiesektor in Deutschland ist ein interessantes Ziel für Hacker. CyberKriminelle, Hacker und staatlich finanzierte Akteure haben heute die Motive und die Fähigkeiten, erfolgreich anzugreifen, um sensible betriebliche und Kundendaten zu stehlen, Unternehmen zu erpressen oder zentrale Kontrollsysteme zu stören oder sogar zu zerstören.

Dies sind nur einige der Bedrohungen, die Benjamin Nawrath den Schlaf rauben. Benjamin Nawrath ist Information Security Officer beim Energieversorger Energie Südbayern (ESB), der Erdgas und Elektrizität für 120.000 Haushalte in Süddeutschland bereit stellt. Als größter regionaler Anbieter beschäftigt ESB ungefähr 350 Angestellte, wobei neben Benjamin Nawrath weitere 14 Mitarbeiter in der IT arbeiten.

Compliance als Last

Eine der größten Herausforderungen für Benjamin Nawrath ist die Einhaltung des deutschen IT-Sicherheitsgesetzes (ITSG), das im Jahr 2015 beschlossen wurde und ab Juli 2017 zur Anwendung kommt. Das Gesetz verlangt von allen Betreibern kritischer Infrastrukturen ein fortschrittliches Cybersecurity-Programm, das die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT-Infrastruktur gewährleisten muss. Es verlangt außerdem, dass Organisationen ihre Compliance regelmäßig zertifizieren lassen. Ein Verstoß kann mit einer Buße von mehreren hunderttausend Euro belegt werden.

In einer großen und komplexen Umgebung (einschließlich 2.000 IP-Adressen), die überwacht werden muss, begrenzten personellen Ressourcen in der IT-Abteilung, einer wachsenden Compliance-Last und hoch motivierten Hackern als Gegnern benötigte Benjamin Nawrath robuste technologische Lösungen, um diesen Herausforderungen erfolgreich zu begegnen.

***Unser preisgekröntes Produkt „Nexpose" wurde zu InsightVM weiterentwickelt. Es nutzt die Leistung der Insight Plattform von Rapid7, unserer Cloud-basierten Lösung für Sicherheit und Datenanalyse. Erfahren Sie mehr unter www.rapid7.com/insightvm.**

030220

Grünes Licht

Die IT von ESB nutzte bereits Nexpose*, die branchenführende SchwachstellenManagement-Lösung von Rapid7. Dementsprechend lag es nahe, das Portfolio mit Rapid7 zu ergänzen. Um den Bedarf nach einer Lösung für Incident Detection and Response zu decken, wurde schnell und unkompliziert ein Proof of Concept (PoC) mit Rapid7 InsightIDR aufgesetzt, um die Qualitäten der Lösung im realen Einsatz zu bestätigen.

„Ich benötigte eine Lösung, die Intelligenz mitbrachte – nicht nur eine technische Lösung für Regeln. Ich kaufe die Intelligenz, nicht die Regeln. Das war der große Erfolgsfaktor für Rapid7 für uns bei dieser Evaluierung," sagt Benjamin Nawrath. „Splunk und andere ähnliche Lösungen sammeln nur die Logs und ich muss diese selbst auswerten. Aber ich möchte wissen, wenn etwas Seltsames oder Ungewöhnliches passiert - und genau das ist, was mir InsightIDR mitteilt. Es war die beste Lösung, die mir die benötigte Intelligenz zu einem vernünftigen Preis bereitstellt."

ESB machen mit der Kombination von InsightVM (der Weiterentwicklung von Rapid7 Nexpose) und InsightIDR – beide gestützt auf die Rapid7 Insight-Plattform – den nächsten Schritt, um branchenführendes Schwachstellen-Management und Incident Detection and Response bereit zu stellen. Benjamin Nawrath stellt fest, dass beide Lösungen sich einfach einrichten und warten ließen und dass sie vereinfachte Verwaltung und zentrale Berichte mit einem einzigen Agent ermöglichen. ESB war einer der Vorreiter bei der Einführung Cloud-basierter Dienste, dementsprechend gab es bei der Bereitstellung keine Engpässe. Und durch den Fokus auf Sicherheit erhielt die Überwachung der IP-Adressen auch vom deutschen Betriebsrat grünes Licht.

Schnellere Reaktion auf Störfälle

InsightIDR spart der IT von ESB Zeit und hilft ihr, viel schneller auf Vorfälle zu reagieren. Mit der Vereinigung von SIEM, User Behavior Analytics (UBA) und Endpoint Detection and Response (EDR) liegt der Schwerpunkt des völlig neu entworfenen InsightIDR auf der frühestmöglichen Erkennung von Angriffen, so dass die Bösewichte keine Zeit haben, sich zu verstecken.

„Ehrlich gesagt gab es überhaupt keinen Incident Response-Prozess, bevor wir InsightIDR einführten. Ich bekam einfach eine E-Mail von einem Anwender, der mir sagte, etwas sei, anders als sonst'. Dann musste ich mich von Hand einarbeiten und Protokolle durchsuchen, was eine Menge Zeit kostete," sagt Benjamin Nawrath. „InsightIDR hat mir dabei geholfen, schneller auf Vorfälle zu reagieren. Es ist sehr einfach zu nutzen und die Agents bieten einen großartigen Einblick."

Benjamin Nawrath nutzt die Funktionen des Live-Dashboard, um fehlgeschlagene Anmeldeversuche von speziellen Usern zu überwachen. „Einer der vielen Vorteile ist, dass ich InsightIDR nicht vorgeben muss, was ein Dienstkonto ist – es erkennt das einfach." ergänzt er.

Das einfach zu verwaltende Portal erlaubt ihm, ungewöhnlich hohe Werte im Blick zu behalten, wenn sich Mitarbeiter aus anderen Ländern remote anmelden oder andere Metriken auf Compliance-Verstöße hindeuten. Warnungen per E-Mail runden das Bild ab und werden zudem an andere Mitglieder des IT-Teams geschickt, so dass auch diese reagieren können, wenn böswillige Handlungen entdeckt werden.

„InsightIDR hat mir dabei geholfen, schneller auf Zwischenfälle zu reagieren. Es ist sehr einfach zu nutzen und die Agents bieten einen großartigen Einblick."

Risikosenkung mit InsightVM

Zur Überwachung einer komplexen IT-Umgebung, einschließlich sensibler industrieller Steuerungssysteme, benötigte Nawrath außerdem Schwachstellen-Management auf höchstem Niveau mit einer engen Integration in InsightIDR. InsightVM von Rapid7 sammelt, überwacht und analysiert automatisch jegliche Schwachstellen im Unternehmensnetzwerk, bietet fortschrittliche Analysen und Berichte, damit Nutzer Risiken priorisieren und abstellen können.

Bei ESB wird Erfolg durch Risikoreduzierung definiert - eine Aufgabe, bei der sich InsightVM als hervorragend erwiesen hat.

„Ich prüfe regelmäßig und bekomme schon mit Benutzerrechten so viel Informationen, wie ich benötige. Wir haben fast keine Fehlalarme, was großartig ist," sagt Benjamin Nawrath. „InsightVM hilft uns zudem bei der Identifikation alter Systeme, die erneuert, aktualisiert oder sogar abgeschaltet werden müssen. Wir erhalten einen großartigen Einblick in die Risikoevaluierung. Es ist schön zu sehen, wie das Risiko sinkt, wenn wir Gegenmaßnahmen ergreifen."

Die Agents sparten zudem Zeit bei regulären Scans. Der Vorteil der engen Integration mit InsightIDR erlaubt einen großen Effizienzgewinn durch hoch akkurate Korrelationen zwischen Sicherheitsereignissen und Schwachstellen.

Ausblick

Unter dem Strich spart die geballte Leistung von InsightIDR und InsightVM Benjamin Nawrath 60% seiner Zeit. Das wiederum erlaubt ihm mehr Zeit für die Verifizierung der Schwachstellen selbst und die Vorbereitung einer bevorstehenden OSCP-Prüfung. Darüber hinaus konnte er mit den von Rapid7 erzeugten Daten seine Position in der Organisation festigen.

„Das Top-Management hat wenig mit dem Thema IT-Sicherheit zu tun, aber dank beider Rapid7-Produkte bin ich in der Lage, sie von der tatsächlichen Risikosituation zu überzeugen. Ich erhalte dafür mehr Respekt für meine Arbeit," sagt er. „Und da die Lösungen nicht so teuer waren, war es kein Problem, das notwendige Budget zu bekommen."

Für die Zukunft plant Benjamin Nawrath die Implementierung des Remediation Project von InsightVM. Damit kann er Aufgaben an seine Kollegen delegieren. Hauptsächlich aber, so ist er sich sicher, wird die Kombination aus InsightIDR und InsightVM den notwendigen Schutz bieten, der für die Auflagen des IT-Sicherheitsgesetzes notwendig ist – und ESB damit in den kommenden Jahren sicher und compliant halten.