Incident Response – Workshop zum korrekten Verhalten im Ernstfall

Stefan Becker · Till Kleinert

Bundesamt für Sicherheit in der Informationstechnik
{stefan.becker | till.kleinert}@bsi.bund.de

Zusammenfassung

70 Prozent der deutschen Unternehmen und Institutionen waren in den Jahren 2016/2017 von Cyber-Angriffen betroffen – so lautete eines der Ergebnisse der Cyber-Sicherheits-Umfrage 2017. Jede zweite erfolgreiche Cyber-Attacke sorgte dabei für Produktions- bzw. Betriebsausfälle. Auch sabotierte Systeme und Webseiten zählten zu den häufigsten Auswirkungen. Um im Fall der Fälle richtig reagieren zu können, sollten die Verantwortlichen in Unternehmen stets Notfallpläne zur Hand haben und das richtige Verhalten regelmäßig üben. Die Allianz für Cyber-Sicherheit lädt alle interessierten Tagungsbesucher in den Workshop „Incident Response – Korrektes Verhalten im Ernstfall“ ein, um hier Good Practices für die Reaktion auf Cyber-Angriffe zu erarbeiten. Geleitet wird die Session von Stefan Becker, der als ehemaliger Cybercrime-Ermittler seine Erfahrungen aus zahlreichen Verfahren einfließen lässt.

1 Ausgangslage

Im Zuge der immer weiter voranschreitenden Digitalisierung und Vernetzung sind viele Prozesse und Gegenstände des Alltags zu potenziellen Zielen für Cyber-Angriffe geworden. Insbesondere Unternehmen, mit immer neuen externen IT-Schnittstellen zu Produktionssteuerungen, E-Procurement-Systemen und vielen weiteren über das Internet erreichbaren Diensten, geraten dadurch in das Fadenkreuz von Cyber-Kriminellen: Einerseits eröffnen sich hier attraktive Optionen zur Sabotage, Erpressung und Spionage, andererseits aber auch immer mehr Einfallstore für Angriffe. Während früher insbesondere „klassische IT-Systeme“, wie z. B. Arbeitsplatzrechner, Server oder Router, im Fokus standen, schafft u.a. der Bereich „Internet of Things“ zahlreiche neue Möglichkeiten für die Täter.

Der technische Fortschritt wird so gleichzeitig zu einer immer größeren Herausforderung für IT-Sicherheitsverantwortliche. Verschiedene Angriffsszenarien müssen durchdacht und Notfallpläne bereitgehalten werden, um bei Eintritt eines sog. Incidents die richtigen Schritte einleiten und das Tagesgeschäft möglichst unbeeinflusst lassen zu können.

2 Beispiel eines fiktiven Angriffs

Grundlage des Workshops ist das folgende Fallbeispiel. Die Teilnehmer steigen hier in die Diskussion ein, prüfen verschiedene Optionen und entwickeln im Laufe der Veranstaltung einen Lösungsweg.

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 329-332.

Im Laufe eines Freitagvormittags erhält Ihr Unternehmen ein Einschreiben. Der Absender droht damit, wichtige IT-Systeme in Ihrer Organisation dauerhaft zu stören und essenzielle Daten zu manipulieren. Beigefügt ist einerseits eine Zahlungsaufforderung in Höhe von 100 Bitcoins, andererseits ein Link zu einer Webseite mit weiterführenden Informationen. Dort läuft ein Countdown bis zum darauffolgenden Dienstag, 12 Uhr. Der oder die Täter drohen damit, Ihr Unternehmen nach Ablauf der Frist lahm zu legen und auf Ihrer Unternehmenswebseite Falschmeldungen zu platzieren, die den Aktienkurs in den Keller treiben könnten. Im Laufe der nächsten Tage sollen außerdem vereinzelte, leichtere Angriffe erfolgen, um die Ernsthaftigkeit der Situation zu unterstreichen.

Ihre IT-Abteilung stellt in den darauffolgenden Stunden verschiedene Netzwerkanomalien fest. Es ist demnach davon auszugehen, dass das Erpresserschreiben echt ist.

Am Freitagnachmittag um 15 Uhr verleihen der oder die Täter ihrem Vorhaben erstmals Nachdruck: die Geschwindigkeit des Firmennetzwerks verringert sich spürbar, Netzwerkdrucker und zentrale Dienste sind nicht mehr erreichbar. In der Folge klingeln die Telefone des IT-Supports in Dauerschleife, weil Mitarbeiter in ihrer Arbeit beeinflusst werden.

Ihre Situation wird durch das bevorstehende Wochenende spürbar begünstigt, da – abgesehen vom einzurufenden Krisenstab – um 18 Uhr der letzte Mitarbeiter nach Hause geht.

Ihnen stehen nun ereignisreiche Tage bevor. Wie gehen Sie vor?

2.1 Start der Ermittlungen

Um die Behandlung des Incidents einleiten zu können, müssen zunächst sämtliche Stakeholder informiert und möglichst in den Krisenstab miteinbezogen werden. Hierzu zählen nicht nur IT-Experten. Auch Vertreter aus Öffentlichkeitsarbeit oder Juristen können Interesse an einer Mitwirkung haben. Die Kontaktaufnahme zur Polizei sollte selbstverständlich sein. Sofern nicht hausintern vorhanden, empfiehlt sich außerdem die Einbestellung externer IT-Sicherheitsdienstleister, wie z.B. IT-Forensikern.

Ein Incident Response Team kann somit aus folgenden Funktionen bestehen:

- IT-Sicherheitsverantwortlicher
- IT-Administrator
- IT-Forensiker
- Geschäftsführung
- Mitarbeiter der Öffentlichkeitsarbeit
- Juristen
- Datenschutzbeauftragte – sofern nicht in Personalunion mit den Juristen
- Sofern notwendig: Kontaktpersonen bei externen Dienstleistern
- …

Im Anschluss steht eine Eingrenzung im Vordergrund, welche Bereiche des Unternehmensnetzwerks bereits kompromittiert wurden und welche Gegenmaßnahmen zur Verfügung stehen. Hier eignen sich z.B. folgende Fragestellungen:

- Was hat der Angreifer auf dem System gemacht?

- Wer hatte unberechtigten Zugang?
- Zu welchem Zeitpunkt fand der Vorfall statt?
- Welche Systeme sind betroffen?
- Warum ist gerade dieses Netz oder System angegriffen worden?
- Wie konnte der Angreifer Zugriff erlangen?
- Ist der Angriff vor kurzem geschehen? Was macht der Angreifer jetzt?
- Was konnte der Angreifer auf diesem/von diesem System einsehen?
- Hat der Angreifer etwas zurückgelassen?

3 Korrektes Verhalten im Ernstfall

Auf die im Fallbeispiel beschriebenen Entwicklungen kann wesentlich entspannter reagiert werden, wenn das Verhalten im Ernstfall vonseiten des Unternehmens bereits im Vorfeld durchdacht wurde. Ein Notfallplan eignet sich, um angemessen auf einen Incident reagieren zu können. Hier sollten bereits im Vorfeld die notwendigen Schritte identifiziert und vorbereitet worden sein. Wie dies gelingen kann, soll das Thema des Workshops sein. Zu den Diskussionspunkten zählen insbesondere:

3.1 Verantwortlichkeiten klären

Wer ist in einer Organisation für welche Geschäftsbereiche und Prozesse zuständig? Welche Abteilungen müssen bei der Bewältigung eines Vorfalls miteinbezogen werden? Wer sind die relevanten Ansprechpartner bei externen Dienstleistern, deren Systeme bei dem Cyber-Angriff in Mitleidenschaft gezogen wurden? Diese Themenkomplexe gehören zu dem Fragenkatalog, mit dem sich ein IT-Sicherheitsverantwortlicher regelmäßig beschäftigen sollte. Hier reicht es nicht, die entsprechenden Kontaktdaten einmalig zu sammeln. Insbesondere bei externen Dienstleistern kann es vorkommen, dass Personalwechsel stattfinden, die neuen Ansprechpartner aber nicht beim Unternehmen hinterlegt werden. Um bei einem Incident stets valide Kontaktdaten vorliegen zu haben, ist also eine regelmäßige Überprüfung notwendig. Wie dies effizient geregelt werden kann, soll auch Thema des Workshops sein.

3.2 Notfallkonzept entwickeln, bereithalten und üben

Notfallkonzepte liefern den Beteiligten bei Sicherheitsvorfällen hilfreiche Anleitungen, um das Ausmaß zu minimieren und den Normalbetrieb schnellstmöglich wieder aufnehmen zu können. Der Workshop wird der Frage nachgehen, welchen Umfang ein Notfallkonzept braucht und wie dieses archiviert werden sollte, denn – soviel sei vorab verraten – es empfiehlt sich nicht, das Dokument auf einem Netzlaufwerk oder auf der lokalen Festplatte vorzuhalten. Dieses Vorgehen führt bspw. bei einem Ransomware-Befall schnell zur Nicht-Verfügbarkeit eines derartigen Notfallplans.

Elementar für die effiziente Bearbeitung eines Vorfalls ist außerdem ein eingespieltes Team. Aufgrund dessen sollte das Verhalten bei einem Incident regelmäßig geübt werden. Vorgehensweisen und Beispielinhalte einer solchen Übung werden ebenfalls im Workshop behandelt.

4 Ausblick

Sofern Sie das Thema im Nachgang zum Workshop in Ihrer Institution vertiefen möchten, empfehlen wir Ihnen die Hinweise des Bundesamtes für Sicherheit in der Informationstechnik – insbesondere den BSI-Standard 100-4 „Notfallmanagement“: http://bsi.bund.de/grundschutz

Eine modernisierte Fassung ist aktuell in Arbeit. Bei Fragen, Problemen oder Anregungen stehen Ihnen die Autoren des Beitrags gerne zur Verfügung.

Literatur

[BSI17] Bundesamt für Sicherheit in der Informationstechnik: "Cyber-Sicherheits-Umfrage 2017". https://www.allianz-fuer-cybersicherheit.de/AC S/D E/Informationspool/CyberSicherheitsUmfrage_2017/CS_Umfrage_2017_node.html (abgerufen am 26.7.2018)

[BSI08] Bundesamt für Sicherheit in der Informationstechnik: "BSI-Standard 100-4: Notfallmanagement". Bundesanzeiger Verlag, 2008, ISBN: 978-3-89817-693-4. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard04/ITGStandard04_node.html (abgerufen am 26.7.2018)

[BaFr17] M. Bartsch, S. Frey: "Cyberstrategien für Unternehmen und Behörden – Maßnahmen zur Erhöhung der Cyberresilienz". Springer Vieweg, Wiesbaden 2017, ISBN: 978-3-658-16138-5.