Weber, Kristin; Schütz, Andreas E.; Fertig, Tobias

Insider Threats – Der Feind in den eigenen Reihen

HMD Praxis der Wirtschaftsinformatik

Provided in Cooperation with:
Springer Nature

Suggested Citation: Weber, Kristin; Schütz, Andreas E.; Fertig, Tobias (2020) : Insider Threats – Der Feind in den eigenen Reihen, HMD Praxis der Wirtschaftsinformatik, ISSN 2198-2775, Springer Fachmedien Wiesbaden, Wiesbaden, Vol. 57, Iss. 3, pp. 613-627, https://doi.org/10.1365/s40702-020-00616-9

HMD (2020) 57:613–627
https://doi.org/10.1365/s40702-020-00616-9

SCHWERPUNKT

Insider Threats – Der Feind in den eigenen Reihen

Kristin Weber · Andreas E. Schütz · Tobias Fertig

Eingegangen: 21. Februar 2020 / Angenommen: 4. April 2020 / Online publiziert: 16. April 2020

Zusammenfassung Eine große Bedrohung für die Informationssicherheit geht von Mitarbeitern aus, die absichtlich der eigenen Organisation schaden wollen. Mitarbeiter besitzen Zugriffsrechte für sensible Informationen und genießen das Vertrauen des Unternehmens. Werden sie allerdings aufgrund persönlicher Motive oder äußerer Umstände zu Whistleblowern, Spionen, Betrügern, Saboteuren, Malicious Enablern oder Datendieben, können sie großen Schaden anrichten. Dieser Artikel untersucht die Motive sogenannter Malicious Insider und stellt die sechs verschiedenen Typen anhand von realen Beispielen der jüngeren Vergangenheit vor. Er zeigt, welche erkennenden, präventiven und reaktiven Maßnahmen Organisationen ergreifen sollten, um die Risiken durch Attacken von böswilligen Insidern zu minimieren. Der Fokus liegt auf den erkennenden Maßnahmen. Durch frühzeitiges Eingreifen werden Mitarbeiter gar nicht erst zu Malicious Insidern. Eine Kombination aus persönlicher Veranlagung (z. B. Introversion, Gier, Kritikunfähigkeit), Stressfaktoren (z. B. Frustration, Unzufriedenheit) und auffälligem Verhalten (z. B. außergewöhnliche Arbeitszeiten oder Reiseziele) weist häufig auf potentielle Täter hin.

Schlüsselwörter Insider Threats · Informationssicherheit · Malicious Insider · Whistleblowing

K. Weber (✉) · A. E. Schütz · T. Fertig
Fakultät Informatik und Wirtschaftsinformatik, Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt, Sanderheinrichsleitenweg 20, 97074 Würzburg, Deutschland
E-Mail: kristin.weber@fhws.de

Insider Threats – Hidden Enemies

Abstract Employees that intentionally want to harm their organization pose a major threat to information security. Employees have access rights to sensitive information, and their organization trusts them. However, they can substantially harm their organization, if they become Whistleblowers, Spies, Scammers, Saboteurs, Malicious Enablers, or Data Thieves due to different personal motives or external circumstances. This paper analyzes motives of so-called Malicious Insiders. It introduces the six types of Malicious Insiders by showing real cases from the recent past. The paper lays out which recognizing, preventive, and reactive measures organizations can take in order to minimize the risks associated with insider threats. The focus is on recognizing potential Malicious Insiders, because through early intervention, employees might not become malicious first. A combination of personal predispositions (e.g., introversion, greed, inability to accept criticism), stressors (e.g., frustration, dissatisfaction), and concerning behavior (e.g., unusual working hours or travel destinations) often points towards potential offenders.

Keywords Insider Threats · Information Security · Malicious Insider · Whistleblowing

1 Gefahr von Insider-Attacken

Die Rolle der Mitarbeiter in Bezug auf Informationssicherheit ist kontrovers. Mitarbeiter können sich als eine große Stütze für das Informationssicherheitskonzept erweisen, stellen jedoch auch eine der größten Bedrohungen für sensible Informationen und Informationstechnik in Organisationen dar. Eine einzelne Person kann großen Schaden anrichten, wenn sie mit den nötigen Rechten und dem Wissen über Prozesse und Strukturen ausgestattet die eigene Organisation angreift. Die Konsequenzen von Insider-Attacken reichen von Reputationsverlust und Datenschutzverletzungen, über finanzielle Einbußen und Schäden an der IT-Infrastruktur bis zum Verlust geistigen Eigentums.

Laut einer Studie werden weltweit mehr Cyberattacken auf Unternehmen durch Angestellte oder Dritte mit Systemzugriff durchgeführt (60 %) als durch externe Angreifer (40 %) (Brandt 2016). Etwa ein Sechstel der Angriffe sind auf Anwenderfehler oder unbedachte Mitarbeiter zurückzuführen. Fast die Hälfte der Angriffe wurde jedoch absichtlich, also mit einem böswilligen Motiv, durch sogenannte Malicious Insider durchgeführt. Weitere Studien kommen zu ähnlichen Ergebnissen (McClimans et al. 2016; Blankenship and O'Malley 2019): Von den befragten Sicherheitsexperten gab über die Hälfte an, in den vergangenen zwölf Monaten versuchten oder erfolgreichen Datendiebstahl sowie Korruption durch Unternehmensinsider erlebt zu haben.

Die Gefahr durch böswillige Insider ist für Unternehmen deshalb so groß, weil die meisten Sicherheitsmaßnahmen keinen Schutz bieten. Selbst starke Verschlüsselungen sind machtlos, wenn die Täter aufgrund ihrer Position über legale Zugriffsrechte verfügen und diese missbräuchlich verwenden.

Dieser Artikel beschäftigt sich mit Malicious Insidern und den durch sie ausgehenden Gefahren. Damit Organisationen frühzeitig böswillige Insider entdecken und sich erfolgreich gegen diese wehren können, müssen mögliche Motive der Insider bekannt sein (Blankenship and O'Malley 2019). Daher legt dieser Artikel im ersten Teil den Fokus auf die Beschreibung unterschiedlicher Insider-Typen und deren Motive für ihre schadhaften Handlungen.

Das folgende Kapitel erläutert anhand verschiedener Ansätze den Begriff Insider und grenzt ihn von Malicious Insidern ab. Das darauffolgende Kapitel beschreibt dann die verschiedenen Typen solcher böswilligen Insider und führt Vorfälle der jüngeren Vergangenheit zu Malicious Insidern als Beispiele an. Das abschließende Kapitel zeigt, wie sich Organisationen mit erkennenden, präventiven und reaktiven Maßnahmen gegen Malicious Insider schützen können.

2 Insider

Aus Sicht des *Information Security Managements* kann der Grad der Beteiligung eines Akteurs an der Informationsverarbeitung und -speicherung einer Organisation als „Insiderness" bezeichnet werden. Ein Insider überschreitet demnach eine bestimmte logische oder physische Begrenzung einer Organisation und kennt dadurch deren innere Umgebung. Insider können also bspw. Mitarbeiter, Vertragspartner, Kunden, Lieferanten oder Berater sein. Einem Insider wird meist erweiterter Zugang zu Informationen gewährt. Von diesem Akteur wird erwartet, dass er sich in einer bestimmten Weise verhält: ihm wird im Umgang mit Informationen vertraut. Die individuelle Motivation des Akteurs ist ausschlaggebend, damit er sich wie erwartet verhält.

Auf ein *IT-System* bezogen ist ein Insider eine Person mit privilegiertem Zugang zu diesem System. Als Insider können demnach Personen bezeichnet werden, die Wissen über ein IT-System besitzen – also auch Personen, die am Design und an der Implementierung des Systems beteiligt waren, aber nicht mehr Teil der Organisation sind (Hunker and Probst 2011).

Unter einem *betriebswirtschaftlichen Ansatz* definiert sich ein Insider dadurch, dass er die Fähigkeit besitzt, eine Organisation gegenüber Außenstehenden zu repräsentieren (Hunker and Probst 2011). Ein Insider hat auch das Recht auf Vermögenswerte der Organisation zuzugreifen und diese entsprechend seiner Tätigkeit einzusetzen.

Insider können auch anhand der von ihnen ausgehenden *Bedrohungen* für eine Organisation definiert werden (Probst et al. 2010). Insider werden als eines der schwierigsten Probleme für die Informationssicherheit angesehen, weil diese Personen Informationen und Möglichkeiten besitzen, die externe Angreifer nicht besitzen. In diesem Zusammenhang können zwei Insider-Bedrohungen unterschieden werden:

- Insider, die dem Unternehmen ohne Absicht und ohne ihre Kenntnis Schaden zufügen – Unintentional oder Accidential Insider.
- Insider, die ihrer Organisation mit abweichendem Verhalten bewusst und gewollt Schaden zufügen – Intentional oder Malicious Insider.

Das Erkennen und die Abwehr von Accidential und Malicious Insiders unterscheiden sich erheblich. Das Abstellen von unabsichtlichem Fehlverhalten kann durch Sensibilisierungsmaßnahmen erreicht werden und fällt in den Bereich der Information Security Awareness (vgl. Weber et al. 2019). Im Folgenden wird nur noch Bezug auf Malicious Insider genommen.

Malicious Insider sind sich bewusst, dass ihre Handlungen Schaden verursachen. Ihre Handlungen sind also böswillig. Ihre Absichten können hingegen aus ihrer Sicht gutwillig sein. Doch sobald die Personen mit ihren bewussten Handlungen Schaden anrichten, können sie als Malicious Insider angesehen werden (McGough et al. 2015).

Ein Malicious Insider kann als ein aktueller oder ehemaliger Mitarbeiter, Vertragspartner oder Geschäftspartner angesehen werden, der Zugriff auf das Netzwerk, Systeme oder Daten hat oder gehabt hat. Dieser Zugriff wird absichtlich missbraucht, sodass die Integrität, Vertraulichkeit oder Verfügbarkeit der Informationen oder Informationssysteme der Organisation, die den Zugang gewährt, beeinträchtigt wird (Cappelli et al. 2012).

Aufgrund der Tatsache, dass Insider die Organisation kennen, kann es schwierig sein, deren Angriffe zu erkennen. Dies liegt unter anderem daran, dass sie ihre Spuren leicht entfernen bzw. so agieren können, dass keine Spuren entstehen.

3 Typen von Malicious Insidern

Dieses Kapitel stellt verschiedene Typen von Malicious Insidern vor. Die Gliederung erfolgt anhand der Motivation eines Insiders, der eigenen Organisation Schaden zuzufügen.

Tab. 1 zeigt eine Zusammenfassung möglicher Motive (Murphy 2019; Blankenship and O'Malley 2019) und ordnet sie den Insidertypen zu.

Tab. 1 Zusammenfassung von Motiven und deren Zuordnung zu Insidertypen

Motivation	Beschreibung	Insidertyp
Finanzielle Notlage	Insider versuchen aufgrund finanzieller Probleme schnell an Geld zu kommen	Datendiebstahl, Betrug, Enabling
Anspruchsrecht	Manche Mitarbeiter denken, sie haben berechtigten Anspruch auf sensible Informationen oder geistiges Eigentum	Datendiebstahl
Verärgerte Mitarbeiter	Mitarbeiter, die sich schlecht behandelt fühlen, wollen sich an ihrem Arbeitgeber rächen	Sabotage
Ideologie	Politische oder religiöse Ansichten können Insider motivieren, böswillig zu handeln	Whistleblowing, Spionage
Äußerer Einfluss	Kriminelle Organisationen oder Geheimdienste rekrutieren Insider, motivieren sie finanziell oder setzen sie mit Drohungen unter Druck	Spionage, Sabotage, Enabling

3.1 Whistleblowing

Whistleblowing bezeichnet im Allgemeinen Personen, die geheime Dokumente oder aus ihrer Sicht unmoralische Praktiken einer Organisation offenlegen. Aus Sicht der Geschädigten führen Whistleblower böswillige Handlungen durch und verfolgen dabei schlechte Absichten. Die Absicht der Whistleblower ist, aus ihrer eigenen Sicht, gutwillig, auch wenn sie sich bewusst sind, dass ihre Handlungen für die Organisation schlecht sind (McGough et al. 2015).

Den Whistleblowern fehlt die Macht, die Prozesse einer Organisation selbst oder auf einem anerkannten Weg zu ändern. Sie ziehen deshalb andere Instanzen, meist die Öffentlichkeit, hinzu. Die größte Motivation der Whistleblower, die Informationen zu veröffentlichen, ist, dadurch Einfluss auf Prozesse oder Praktiken der Organisation zu nehmen.

Einer der bekanntesten Whistleblower ist Edward Snowden. Er war ein US-amerikanischer IT-Sicherheitstechniker, der als Subunternehmer für die National Security Agency (NSA) und die Central Intelligence Agency (CIA) tätig war (Biography.com Editors 2019). Später wechselte Snowden zur Beratungsfirma Booz Allen Hamilton, die ihn als IT-Berater in eine NSA-Einrichtung entsandte. Durch seine Tätigkeit erhielt Snowden erneut Zugriff auf streng geheime Dokumente, welche er nun in großen Mengen kopierte.

Nachdem Snowden große Mengen geheimer Dokumente zusammengestellt hatte, veröffentlichte er seit 2013 über The Guardian und The Washington Post eine Flut von geheimen Dokumenten der geheimdienstlichen Überwachungen. In einem Interview gab Snowden als seine Motivation an: „Ich will nicht in einer Gesellschaft leben, die solche Dinge tut. Ich will nicht in einer Welt leben, in der alles, was ich tue und sage, aufgezeichnet ist. Das ist nichts, was ich unterstützen oder mit dem ich leben will.“ (Greenwald et al. 2013).

3.2 Datendiebstahl

In der Regel wird der Diebstahl von Daten von Ingenieuren, Wissenschaftlern, Programmieren oder Vertriebsmitarbeitern durchgeführt (Kont et al. 2018). Also von genau den Mitarbeitern, die Zugriff auf sensible Informationen einer Organisation besitzen bzw. diese erzeugen.

Die Art, wie der Diebstahl erfolgt, kann sehr unterschiedlich sein. Physische Dokumente können aus Unternehmensgebäuden entwendet oder Daten auf einem Datenträger an einen anderen Ort befördert werden. Elektronische Prozesse, wie zum Beispiel das Versenden einer E-Mail oder der Upload auf Cloud-Speicher, erleichtern das unberechtigte Entwenden von Daten.

Sowohl Handlung als auch Absicht sind als böswillig einzustufen. Im Gegensatz zu Whistleblowern verfolgen diese Malicious Insider persönliche Ziele. Sie möchten zum Beispiel mit den Informationen und Daten, die sie gestohlen haben, eigene Unternehmen gründen, in einem neuen Job von den Daten profitieren oder diese gegen die ehemalige Organisation einsetzen (AO Kaspersky Lab 2020). Auch die Daten, die gestohlen werden, sind sehr unterschiedlich. Häufig werden proprietärer

Software- und Source-Code, strategische Unternehmenspläne oder Produkt- und Kundeninformationen entwendet (Cappelli et al. 2012).

Ein spektakulärer Datendiebstahl wurde von Anthony Levandowski begangen. Levandowski war Mitarbeiter bei Google und Mitbegründer von Otto, einer Firma, die selbstfahrende Trucks entwickelt und von Uber übernommen wurde (Harris 2017). Levandowski arbeitete in mehreren Projekten von Google, unter anderem Street View, Kitty Hawk und Googles fahrerlose Autos (später Waymo). Waymo verklagte Uber, weil Uber proprietäre Technologien gestohlen und die Patente der Firma Waymo verletzt haben soll. In der Klage wird Levandowski beschuldigt, wenige Wochen vor seinem Rücktritt bei Google mehr als 14.000 höchst vertrauliche Dateien auf ein externes Laufwerk heruntergeladen und somit gestohlen zu haben. Die Daten sollen Informationen über Techniken enthalten, die sowohl Waymo als auch Uber für ihre selbstfahrenden Testfahrzeuge verwenden (Mac et al. 2017).

3.3 Spionage

Spione möchten zugunsten einer anderen Organisation oder eines Staates bedeutsame Informationen oder geschütztes Wissen erbeuten, damit die Auftraggeber diese für ihre Zwecke nutzen können. Spionage kann sowohl von technisch versierten als auch technisch nicht versierten Mitarbeitern ausgeführt werden. In der Regel findet Spionage über einen längeren Zeitraum statt.

Im Gegensatz zu den meisten Whistleblowern zeichnen sich Spione dadurch aus, dass sie im Geheimen operieren (Kont et al. 2018). Der Unterschied zum Datendiebstahl besteht darin, dass Spione in der Regel im Auftrag anderer Personen handeln. Auch die Gründe lassen Unterschiede zum Datendiebstahl erkennen. Das Kürzel MICE zeigt die Motive von Spionen (Becker et al. 2014): Spione handeln entweder aus finanziellen Gründen (Money), wegen ihrer Überzeugung oder einer Ideologie (Ideology), weil sie dazu gezwungen sind (Coercion) oder aufgrund der daraus resultierenden Selbstwahrnehmung und um sich von anderen Personen abzuheben (Ego).

Ein aus China stammender Ingenieur wurde in den Vereinigten Staaten von Amerika wegen Wirtschaftsspionage zu 15 Jahren Gefängnis verurteilt. In den späten 1970er Jahren, nachdem er vom damals führenden Konzern für Luft- und Raumfahrt Rockwell-International angeheuert wurde, begannen seine Spionage-Aktivitäten für die Volksrepublik China (Mail Foreign Service 2009). Der Täter hielt Präsentationen in China, schickte Informationen über seine Arbeit per Diplomatengepäck nach China und sammelte über 300.000 geheime Dokumente über Raumfahrt- und Militärprogramme der USA in seinem Keller. Der Täter sah die Möglichkeit, durch seine Spionage-Aktivitäten einen Teil zum wirtschaftlichen Fortschritt seines Heimatlandes China zu leisten. 2006 entdeckten Staatsanwälte in den USA bei der Untersuchung eines Spionagefalls eine Spur, die schließlich zum Täter führte.

3.4 Sabotage

Besonders technisch versierte Mitarbeiter können der eigenen Organisation durch die Sabotage von Systemen einen erheblichen Schaden zufügen (Kont et al. 2018).

Im Gegensatz zu Spionen versuchen Saboteure der Organisation aus persönlichen Gründen zu schaden (AO Kaspersky Lab 2020). Sowohl die Handlungen als auch die Absichten eines Saboteurs sind böswillig.

Studien belegen, dass die meisten Saboteure gerade die Systeme sabotieren, die sie täglich nutzen – obwohl es deren Aufgabe ist, diese am Laufen zu halten. Typische Motive für Sabotage sind Frustration, Rache, mangelnde Wertschätzung und das Gefühl der Machtlosigkeit gegenüber einer vermeintlich ungerechten Behandlung (Kont et al. 2018; Noonan 2018).

Die meisten Sabotage-Aktionen werden vorbereitet, während die Mitarbeiter noch Teil der Organisation sind. Die Ausführung erfolgt kurz bevor oder sobald die Insider die Organisation verlassen (Cappelli et al. 2012).

Ein Beispiel für einen Sabotageakt liefert ein ehemaliger IT-Mitarbeiter einer kanadischen Eisenbahngesellschafft, der von seinem Arbeitgeber entlassen wurde. Bevor er seinen Laptop und seinen Ausweis zurückgab, verschaffte er sich Zugriff zu zentralen und kritischen Switches der Firma. Er sabotierte die Netzwerk-Geräte, entfernte Konten auf administrativer Ebene und änderte die Zugangsdaten für die verbliebenen Administrator-Konten. Nur durch einen riskanten Neustart konnten die Administratoren den Zugriff auf die Geräte zurückerlangen. Die Racheaktion an seinem ehemaligen Arbeitgeber durch Insiderwissen brachte dem Täter eine einjährige Gefängnisstrafe wegen absichtlicher Sabotage des Computernetzwerkes ein (U.S. Attorney's Office 2018).

3.5 Betrug

Unter Betrug wird vorsätzliche Täuschung verstanden, um einen rechtswidrigen oder unberechtigten Nutzen zu erwirken (Noonan 2018). Betrug nimmt viele Formen an, u. a. Identitätsdiebstahl, Wirtschaftskriminalität und Marktmanipulation. Betrug findet häufig über einen längeren Zeitraum statt und wird von finanziellen Anreizen oder Gier getrieben (Cappelli et al. 2012). Eine weitere Motivation besteht darin, die eigene Position innerhalb einer Organisation auf Kosten anderer oder auf Kosten der Organisation zu verbessern. So könnten Mitarbeiter ihre Personalakte ändern, um höhere Chancen auf eine Beförderung zu haben (McGough et al. 2015).

Ein ehemaliger Angestellter einer Sicherheitsfirma, der nach seinem freiwilligen Rücktritt verschiedene Angriffe auf seinen ehemaligen Arbeitgeber durchführte, beging dabei Betrug und Sabotage. Mithilfe einer Fernzugriffssoftware, die er während seiner aktiven Zeit installierte, verschaffte sich der Angestellte nach seinem Austritt Zugriff auf den Computer des Betriebsleiters und erbeutete Passwörter sowie weitere Zugangsdaten. Er löschte unter anderem Dateien, wie zum Beispiel Personalakten und Zeitpläne sowie Kundeninformationen, er verschickte vom Account des Betriebsleiters böswillige E-Mails an Kunden der Firma und lenkte alle Besucher der Website der Firma auf die Website eines Konkurrenten um (Burgess 2017). Als Grund für seine Taten konnten ein starkes Alkohol- und Drogenproblem und eine schwierige Kindheit ausgemacht werden (Murdock 2017). Der Täter wurde zu sieben Jahren Haft verurteilt.

3.6 Malicious Enabling

Mitarbeiter führen Angriffe nicht immer selbst durch. Wenn sie die Voraussetzungen dafür schaffen, dass externe Angreifer Attacken durchführen, wird diese Begünstigung eines Angriffs als Malicious Enabling bezeichnet. Neben der bewussten Weitergabe von Zugangsdaten oder der Offenlegung von Netzwerkarchitekturen, kann auch das bewusste Implementieren einer Hintertür als Malicious Enabling angesehen werden. Diese Hintertür nutzt der Angreifer, um die Zugangskontrollen der Organisation zu umgehen.

Ein Beweggrund für Enabling kann die grundsätzliche Bereitschaft, aber fehlendes technisches Knowhow für einen Angriff sein. Somit nutzen die Insider ihre Stellung aus, um die Möglichkeit Schaden anzurichten, an jemand anderen weiterzugeben. Gleichzeitig kann der Antrieb, als Malicious Enabler unentdeckt zu bleiben, eine wichtige Rolle spielen. Ein Insider kann zudem von einer Person außerhalb der Organisation dazu beauftragt worden sein, Enabling-Aktionen durchzuführen.

Im Allgemeinen kann die Handlung, die ein Malicious Enabler durchführt, als böswillig und bewusst angesehen werden. Die Absicht eines Enablers kann aber auch unfreiwillig sein. Damit könnten jene Fälle bezeichnet werden, in denen Mitarbeiter von externen Personen oder Organisationen erpresst werden, Angriffe auf die eigene Organisation zu ermöglichen.

4 Maßnahmen gegen Malicious Insider

Absolute Informationssicherheit für eine Organisation gibt es nicht. Das gilt auch für den Schutz vor Malicious Insidern. Im Folgenden werden Maßnahmen gezeigt, die den Schaden nach einem Angriff oder das Risiko durch Malicious Insider angegriffen zu werden, reduzieren. Solche Maßnahmen können in erkennende, präventive und reaktive Aktivitäten unterteilt werden. Zudem sollten die Maßnahmen als Teil des übergeordneten Informationssicherheitsmanagements (ISM) verstanden werden. Im Rahmen des ISM sollten Verantwortlichkeiten für diese Maßnahmen definiert und sich wiederholende, kontinuierlich verbessernde Prozesse aufgesetzt werden.

Aufgrund der Besonderheiten und je nach Größe der Organisation empfiehlt es sich, ein speziell geschultes Team aus ein bis drei Mitgliedern zur Bekämpfung von Bedrohungen durch Malicious Insider aufzubauen (Blankenship and O'Malley 2019).

4.1 Erkennende Maßnahmen

„Gefahr erkannt, Gefahr gebannt" heißt ein gängiges Sprichwort, das seine Wahrheit auch im Kontext von Malicious Insider unter Beweis stellt. Wird die Gefahr erkannt, bevor der Schadensfall eingetreten ist, können die Folgen für die Organisation geringgehalten werden. Potentielle Indikatoren, um Malicious Insidern zu erkennen, umfassen persönliche Eigenschaften, verdächtige Verhaltensweisen oder besondere berufliche Ereignisse. Um von diesen Indikatoren auf einen Malicious Insider schließen zu können, sind leistungsfähige Computerprogramme, sensibilisierte

Mitarbeiter und ein verantwortungsvoller Umgang mit Indikatoren und Hinweisen notwendig.

Bestimmte persönliche Eigenschaften eines Mitarbeiters eignen sich als Indikatoren zur Identifizierung eines potentiellen Malicious Insiders. Laut NCCIC (2014) sind Introversion, Gier, ethische Flexibilität, fehlende Loyalität, rebellisches und aggressives Verhalten, Narzissmus, fehlende Empathie, Kritikunfähigkeit, Frustration und Unzufriedenheit einige der potentiellen Merkmale eines Malicious Insiders – insbesondere der durch Anspruchsrecht, Ärger oder Ideologie motivierten Insider.

Malicious Insider können aber auch über verdächtige Verhaltensweisen identifiziert werden (NCCIC 2014; Noonan 2018; Blankenship and O'Malley 2019). Außergewöhnliche Arbeitszeiten oder Netzwerkzugriffe zu auffälligen Zeiten (während des Urlaubs, nachts) können beispielsweise auf ein schädliches Verhalten hinweisen. Auffällig ist auch, wenn sich Personen plötzlich stark für Angelegenheiten außerhalb ihres Zuständigkeitsbereiches interessieren, unnötigerweise sensible Dokumente und Unterlagen kopieren oder ihre Unzufriedenheit über Richtlinien äußern. Auch Mitarbeiter mit einem auffälligen Lebenswandel können als Malicious Insider aktiv werden. Drogen- oder Alkoholmissbrauch, finanzielle Probleme, illegale Aktivitäten, ungewöhnliche Reiseziele, plötzlicher Reichtum, unerwartete Abwesenheiten, psychische Probleme oder feindseliges Verhalten können Warnzeichen sein. Diese Verhaltensweisen treffen insbesondere auf Insider zu, die in finanzieller Notlage sind oder unter äußerem Einfluss stehen (vgl. Tab. 1).

Bestimmte berufliche Ereignisse können Mitarbeiter in Malicious Insider verwandeln. Kündigungen, schlechte Leistungsbewertungen oder Meinungsverschiedenheiten mit Kollegen können Menschen so verärgern, dass sie zum Täter werden (Blankenship and O'Malley 2019).

Die genannten Indikatoren weisen nicht zwingend auf Malicious Insider hin. Nur weil Mitarbeiter introvertiert sind, eine schwierige Zeit durchmachen oder unzufrieden sind, werden sie nicht zwangsläufig zu Tätern. Daher empfiehlt sich eine sensible Vorgehensweise. Neben der Einhaltung von Datenschutz und Arbeitsrecht muss auch darauf geachtet werden, keine Kultur der Überwachung zu schaffen. Verdächtige Mitarbeiter sollten nur bei bewiesenem oder berechtigtem Verdacht hinzugezogen werden. Außerdem sollten die erhobenen Daten über das Nutzerverhalten wirklich ausschließlich dem Schutz der Informationssicherheit dienen.

Zunächst einmal muss aber geklärt sein, was abweichendes Verhalten ist. Eine typische organisatorische Maßnahme ist daher, Richtlinien zu definieren, die gewünschtes und unerwünschtes Verhalten beschreiben. Aus diesen Richtlinien lassen sich Parameter ableiten, die als Basis für eine Verhaltensanalyse dienen können. Erst mit der Festlegung und der Kommunikation des richtigen Verhaltens an die Mitarbeiter, kann ein bestimmtes Verhalten auch als falsch identifiziert werden.

Erkennende Maßnahmen müssen nun die genannten Indikatoren verknüpfen und Heuristiken entwickeln, um Schlüsse auf ein potentiell schadhaftes Verhalten zu ziehen. Anschließend müssen Möglichkeiten zur Messung der Indikatoren und des abweichenden Verhaltens etabliert werden. So kann z. B. der Zugriff auf Daten oder die Wege, wie Daten ausgetauscht werden, überprüft werden. Unter Zuhilfenahme von Machine Learning oder Behavioral Analytics können Nutzerverhalten und Logfiles analysiert werden (Murphy 2019). Für die Sammlung, Aggregation, Korre-

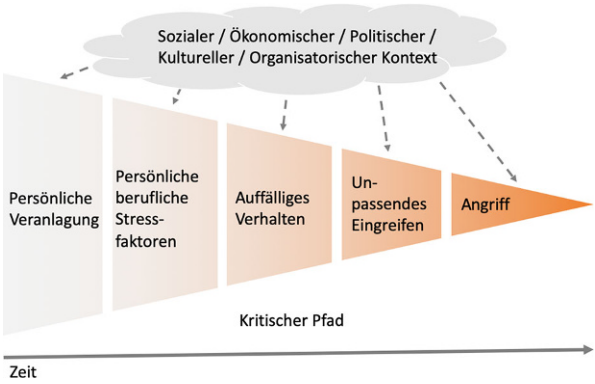

Abb. 1 Der kritische Pfad zum Malicious Insider. (In Anlehnung an Noonan 2018, p. 4.35)

lation und Analyse der großen Datenmenge werden leistungsfähige Tools benötigt, wie z. B. Security Information and Event Management (SIEM). Diese können zudem Heuristiken abbilden und auf potentielle Malicious Insider hinweisen.

Zudem können gezielt Fallen ausgelegt werden (Illusive Networks 2019). Falsche Objekte, wie etwa strategisch bedeutsame Informationen oder Nutzerkennwörter, die das Interesse von Insidern erregen, könnten zugänglich gemacht werden. Sobald der Zugriff eines Malicious Insiders auf die Objekte erfolgt, wird Alarm ausgelöst.

Aber auch die Belegschaft und das Management sollte dazu angehalten werden, wachsam zu sein und gegebenenfalls (anonym) Alarm zu schlagen. Das ist besonders hilfreich, um die Kategorie der verärgerten Mitarbeiter zu identifizieren. Hier kommt Security Awareness ins Spiel. Die Mitarbeiter müssen für die Gefahren von Malicious Insidern und für informationssicherheitskonformes Verhalten sensibilisiert werden (Weber et al. 2019).

Abb. 1 zeigt den Weg auf, wie Mitarbeiter zu Malicious Insidern werden können. Erkennbar sind die Zusammenhänge zwischen persönlicher Veranlagung (oben genannte Indikatoren), Stressfaktoren (berufliche Ereignisse) und auffälligem Verhalten. Weitere Faktoren beeinflussen die Wahrscheinlichkeit für böswilliges Verhalten, z. B. der politische Kontext (vgl. Spionage, Whistleblowing). Zu jedem der genannten Zeitpunkte kann eine erfolgreiche Intervention stattfinden und der „Angriff" gestoppt werden (Noonan 2018).

4.2 Präventive Maßnahmen

Mit „Vorsicht ist besser als Nachsicht" liefert der Volksmund ein passendes Sprichwort für die präventiven Maßnahmen gegen die Gefahren von Malicious Insidern. Solche vorbeugenden Maßnahmen erschweren die Möglichkeit für einen Angriff von Innen bereits im Vorfeld oder verhindern ihn gänzlich. Hierfür sind technische und organisatorische Maßnahmen gleichermaßen entscheidend.

Diese präventiven Maßnahmen werden in Unternehmen häufig in sogenannten Insider Threat Programmen koordiniert. Firmen, die bereits ein solches Programm implementiert haben, setzen dabei vor allem auf folgende Maßnahmen (IS Decisions 2015):

- Erkennen von Insidern durch Technologie bzw. mit speziellen Tools,
- Durchführen von Security Trainings und Awareness Kampagnen für Mitarbeiter und Management,
- Erstellen von Richtlinien,
- Definieren von Verantwortlichkeiten für die Behandlung von Sicherheitsvorfällen,
- Überprüfen von Mitarbeitern vor der Einstellung sowie
- Definieren von Prozessen für das Ausscheiden von Mitarbeitern aus der Organisation.

Dabei zeigt sich, dass viele der organisatorischen Schritte generell Teil eines funktionierenden Informationssicherheitsmanagements sein sollten und nur speziell für die Gefahren von Malicious Insidern angepasst werden müssen.

Für die richtige Auswahl präventiver Maßnahmen müssen Organisationen zuerst verstehen, welche Daten für Malicious Insider überhaupt als potentielles Angriffsziel interessant sind. Im Rahmen des Risikomanagements werden Daten anhand ihres Werts bzw. ihres Risikos bewertet. Das Risiko wird anhand der Auswirkungen bei ungewolltem Abfluss (Bsp. Spionage), Veränderung (Bsp. Betrug) oder Nichtverfügbarkeit (Bsp. Sabotage) eingestuft. Im Fokus stehen bspw. besonders schützenswerte personenbezogene Daten oder Daten, die Organisationen einen Wettbewerbsvorteil verschaffen können. Je nach Wert bzw. Risiko der kritischen Vermögenswerte sind individuelle Schutzmaßnahmen im Rahmen eines Informationssicherheitsmanagementsystems (ISMS) zu definieren. Dabei sollte der Blick explizit nach innen gerichtet und überlegt werden, welchen Vorteil die verschiedenen Typen potentieller Täter durch den Zugriff auf diese Daten haben können.

Grundsätzlich sollte eine effektive Aufgabentrennung erfolgen (Cappelli et al. 2012). So sollte bspw. ein Datenbank-Administrator in keinem Fall derjenige sein, der die Backups für diese Datenbank verwaltet. Das Need-to-Know-Prinzip besagt, dass Personen oder Gruppen nur so viele Zugriffsrechte bekommen, wie für die jeweilige Aufgabe notwendig sind. Nicht nur der Umfang der Rechte, sondern auch die Dauer, wie lange ein solches Zugriffsrecht vergeben wird, sollte bedacht werden. Vor allem sollten nicht länger benötigte Berechtigungen zeitnah gelöscht werden, bspw. auch bei einem Wechsel innerhalb der Organisation.

Mit Data Redaction können sensible Daten maskiert werden (NCCIC 2014). Mit der Maskierung ist nur ein kleiner Teil der Daten sichtbar, der aber ausreicht, um sie zu nutzen. Data Redaction wird bspw. auf Kassenbelegen angewandt, auf denen nur ein Teil der zur Zahlung verwendeten Kartennummer angezeigt wird. Der kleine Teil reicht aus, um später zuzuordnen, welche Karte verwendet wurde – würde aber möglichen Kreditkartenbetrügern, die den Zettel finden, nicht die gesamte Nummer präsentieren.

Weitere präventive Maßnahmen sollten verhindern, dass Mitarbeiter überhaupt zu Malicious Insidern werden (NCCIC 2014). Den Mitarbeitern sollte die Gelegenheit gegeben werden, ihren Frust loszuwerden. Vorgesetzte sollten sensibel mit persönlichen Problemen der Mitarbeiter umgehen und das Gespräch suchen. Mitarbeiter, die sich als Teil des Teams und ernstgenommen fühlen, wollen dem Team keinen Schaden zufügen. In der Organisation sollte eine Kultur herrschen, in der die Mitarbeiter sich gegenseitig helfen und unterstützen.

Noch früher setzt die Maßnahme an, Mitarbeiter vor deren Einstellung, je nach Zugang zu kritischen Informationen, entsprechend zu überprüfen (Noonan 2018). Je nach Art der Organisation gibt es dafür verschiedene rechtlich zulässige Möglichkeiten, wie z. B. Hintergrundüberprüfung, Sicherheitsüberprüfung, Kreditwürdigungsprüfung, Interviews, Sammeln und Auswerten von öffentlich verfügbaren Informationen aus sozialen Medien, Drogentests oder Lügendetektortests. Diese Maßnahmen würden insbesondere Insider enttarnen, die unter äußerem Einfluss stehen, in finanzieller Notlage sind oder unpassende ideologische Ansichten haben (vgl. Tab. 1).

4.3 Reaktive Maßnahmen

„Durch Schaden wird man klug“ heißt eine Redewendung, welche die reaktiven Maßnahmen in diesem Zusammenhang charakterisiert. Haben die erkennenden und präventiven Maßnahmen keine Wirkung gezeigt und der Organisation wurde durch Malicious Insider geschadet, ist es wichtig, richtig zu reagieren. Organisationen stehen dann vor der Aufgabe, Angriffe auf die IT-Systeme oder Informationen des Unternehmens zu analysieren, aufzuklären und den angerichteten Schaden zu beheben. Um einen böswilligen Angriff von innen zu untersuchen, können die Vorgehensweisen der IT-Forensik angewendet werden.

Die Antwort auf einen Angriff von innen muss sehr sorgfältig und wohl überlegt durchgeführt werden. Falsche Anschuldigungen können viele schädliche Auswirkungen auf die Kultur einer Organisation haben (Hunker and Probst 2011). In vielen Fällen kann es durchaus sinnvoll sein, eine anhaltende Insider-Attacke zu dulden und zu beobachten. Oft ist es fataler, die Systeme wegen einer Insider-Attacke abzuschalten, als die Verluste zu akzeptieren und durch die gewonnenen Beweise den Angriff strafrechtlich zu verfolgen (Probst et al. 2010). Da gegen eigene Mitarbeiter vorgegangen wird, ist außerdem wichtig, dass diese Beweise wirklich eindeutig sind (Illusive Networks 2019). Hierfür eignet sich beispielsweise der Einsatz digitaler Wasserzeichen, mit denen elektronische Dokumente forensisch markiert werden können (Waschetzki and Steinebach 2018).

Ein weiterer wichtiger Punkt ist, die Gründe und das Entstehen des Schadens zu reflektieren und den Schadensfall genau zu analysieren. Dabei werden die erkennenden, präventiven und reaktiven Maßnahmen genau überprüft und nach möglichen Schwachstellen und nach Verbesserungspotential in den Abwehrmaßnahmen gesucht. Ebenfalls muss sorgfältig geprüft werden, ob der Vorfall gemäß DSGVO gegenüber den Aufsichtsbehörden meldepflichtig ist. Das wäre bspw. dann der Fall, wenn der Datendiebstahl personenbezogene Daten umfasst.

Wurden im Vorfeld geeignete Maßnahmen zur Wiederherstellung vorbereitet, können diese nach einem Angriff genutzt werden, um wieder zum Normalbetrieb zurückzukehren. Beispiel war hier der Angriff auf das kanadische Eisenbahnunternehmen (vgl. 3.4). Als die Administratoren erkannten, dass ein Angriff stattgefunden hatte, konnten die Zugriffsrechte nur durch einen Neustart wiederhergestellt werden. Wäre dieser schiefgelaufen, wäre eine Rückkehr zum Normalbetrieb nicht mehr möglich gewesen. Daher sollten wiederherstellende Maßnahmen immer rechtzeitig vorbereitet und getestet werden.

5 Fazit

Insider erhalten das Vertrauen ihrer Organisation, das allerdings auch ausgenutzt werden kann. Missbrauchen Insider dieses Vertrauen selbst oder ermöglichen externen Angreifern die Schutzmaßnahmen zu umgehen, kann das weitreichende Folgen für die Verfügbarkeit, Vertraulichkeit und Integrität der Informationen einer Organisation haben.

Nicht alle Malicious Insider sind gleich. Sollen effektive Maßnahmen zum Erkennen von Insidern, zur Prävention und Reaktion von böswilligen Angriffen ergriffen werden, müssen die Gründe der verschiedenen Typen von Malicious Insidern und Motivationen für einen Angriff bekannt sein. Beispielsweise werden verärgerte Mitarbeiter gar nicht erst tätig werden, wenn deren Ärger ernst genommen wird und sie in der Organisation offen darüber sprechen können. Sechs charakteristische Typen von Malicious Insidern sind Whistleblower, Saboteure, Spione, Betrüger, Datendiebe und Enabler. Der Artikel zeigt, dass Organisationen vor allem in erkennende Maßnahmen investieren sollten. Durch Erkennen und rechtzeitiges Eingreifen kann Insider-Attacken vorgebeugt werden.

Die Identifikation von Malicious Insidern muss allerdings behutsam durchgeführt werden. Die einzelnen Maßnahmen können schnell für eine Überwachung der Mitarbeiter missbraucht werden, weshalb diese gezielt und nur bei vorliegendem Verdacht eingesetzt werden sollten. Zusätzlich zu den technischen Identifikationsmaßnahmen eignet sich die Mithilfe der Belegschaft. Durch zielgerichtete Awareness-Kampagnen lässt sich die Aufmerksamkeit der Mitarbeiter steigern, wodurch auffälliges Verhalten schneller bemerkt werden kann. Bevor dieses Verhalten dann zu einem Angriff führt, kann die Organisation gezielt auf die Probleme des Verdächtigen eingehen. Notfalls kann dann auch mit Hilfe von technischen Maßnahmen eine Kontrolle des Verdachts stattfinden.

Funding Open Access funding provided by Projekt DEAL.

Literatur

Attorney's Office US (2018) Former it employee of transcontinental railroad sentenced to prison for damaging ex-employer's computer network. https://www.justice.gov/usao-mn/pr/former-it-employee-transcontinental-railroad-sentenced-prison-damaging-ex-employer-s. Zugegriffen: 12. Jan. 2020

Becker KB, Das Gupta O, Schulte von Drach MC (2014) Agenten, Informanten, Verräter – Ein historischer Überblick von Mata Hari bis zu Günter Guillaume. In: Süddeutsche Zeitung. https://www.sueddeutsche.de/politik/spione-verraeter-1.2040631. Zugegriffen: 12. Jan. 2020

Biography.com Editors (2019) Edward Snowden Biography. In: The Biography.com website. https://www.biography.com/activist/edward-snowden. Zugegriffen: 12. Jan. 2020

Blankenship J, O'Malley C (2019) Best practices: mitigating insider threats—defend your organization against the threats insiders pose. Forrester Research, Cambridge

Brandt M (2016) Cyberattacken meist Insider-Jobs. In: statista. https://de.statista.com/infografik/5001/verursacher-von-cyberattacken-auf-unternehmen/. Zugegriffen: 12. Jan. 2020

Burgess C (2017) Insider wreaks havoc on company—after he resigns. In: CSO. https://www.csoonline.com/article/3206626/insider-wreaks-havoc-on-companyafter-he-resigns.html. Zugegriffen: 12. Jan. 2020

Cappelli D, Moore A, Trzeciak R (2012) The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud). Addison-Wesley, Upper Saddle River

Decisions IS (2015) User security in 2015: the future of addressing insider threat. IS Decisions. https://cdn.isdecisions.com/pdf/future-insider-threat-user-security.pdf. Zugegriffen: 19.02.2020

Greenwald G, MacAskill E, Poitras L (2013) Edward Snowden: the whistleblower behind the NSA surveillance revelations. In: The Guardian. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance?CMP=twt_gu. Zugegriffen: 12. Jan. 2020

Harris M (2017) By Firing Anthony Levandowski, Uber Got Otto on the Cheap. In: IEEE Spektrum. https://spectrum.ieee.org/cars-that-think/transportation/self-driving/turns-out-uber-got-otto-on-the-cheap. Zugegriffen: 12. Jan. 2020

Hunker J, Probst CW (2011) Insiders and insider threats-an overview of definitions and mitigation techniques. J Wirel Mob Networks Ubiquitous Comput Dependable Appl 2:4–27

Illusive Networks (2019) Stopping the attackers you trust. Illusive Networks. https://www.infosecurityeurope.com/__novadocuments/544221?v=636820416740800000. Zugegriffen: 13.01.2020

Kaspersky Lab AO (2020) Recognizing different types of insiders. In: encyclopedia by Kaspersky. https://encyclopedia.kaspersky.com/knowledge/recognizing-different-types-of-insiders/. Zugegriffen: 12. Jan. 2020

Kont M, Pihelgas M, Wojtkowiak J et al (2018) Insider threat detection study. CCDCOE, Tallinn

Mac R, Solomon B, Ohnsmann A (2017) Meet the former Google engineer who allegedly Stole secrets for Uber. https://www.forbes.com/sites/briansolomon/2017/02/23/meet-the-former-google-engineer-who-allegedly-stole-secrets-for-uber-anthony-levandowski/#a8b6ece5c5ea. Zugegriffen: 12. Jan. 2020

Mail Foreign Service (2009) How boeing engineer spied for Chinese for 30 years... and stole secret space shuttle designs. https://www.dailymail.co.uk/news/article-1200339/How-Boeing-engineer-spied-Chinese-30-years--stole-secrets-space-shuttle.html. Zugegriffen: 12. Jan. 2020

McClimans F, Fersht P, Snowdon J et al (2016) The state of Cybersecurity and digital trust 2016. Accenture and HfS Research Ltd. https://www.accenture.com/t20160704T014005Z__w__/us-en/_acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Report-June.pdf#zoom=50. Zugegriffen: 12.01.2020

McGough AS, Alwis S, Wall D et al (2015) Insider threats: identifying anomalous human behaviour in heterogeneous systems using beneficial intelligent software (Ben-ware). In: Proceedings of the 7th ACM CCS international workshop on managing insider security threats MIST '15.. ACM Press, Denver, S 1–12

Murdock J (2017) Ex-employee faces 7 years in prison after hacking into security firm and deleting client data. https://www.ibtimes.co.uk/ex-employee-faces-7-years-prison-after-hacking-into-security-firm-deleting-client-data-1628776. Zugegriffen: 12. Jan. 2020

Murphy I (2019) Remediating the insider threat. Enterprise Times. https://www.infosecurityeurope.com/__novadocuments/589475?v=636923174749130000. Zugegriffen: 13.01.2020

NCCIC (2014) Combating the insider threat. https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf. Zugegriffen: 21.01.2020

Noonan C (2018) Spy the lie—detecting malicious insiders. Pacific Northwest National Laboratory, Richland

Probst CW, Hunker J, Gollmann D, Bishop M (2010) Aspects of insider threats. In: Probst CW, Hunker J, Gollmann D, Bishop M (Hrsg) Insider threats in Cyber security. Springer, Boston, S 1–15

Waschetzki M, Steinebach M (2018) Digitale Wasserzeichen in der Kriminalistik. Datenschutz Datensicherheit 42:69–73. https://doi.org/10.1007/s11623-018-0896-2

Weber K, Schütz AE, Fertig T (2019) Grundlagen und Anwendung von Information Security Awareness: Mitarbeiter zielgerichtet für Informationssicherheit sensibilisieren. Springer, Berlin Heidelberg