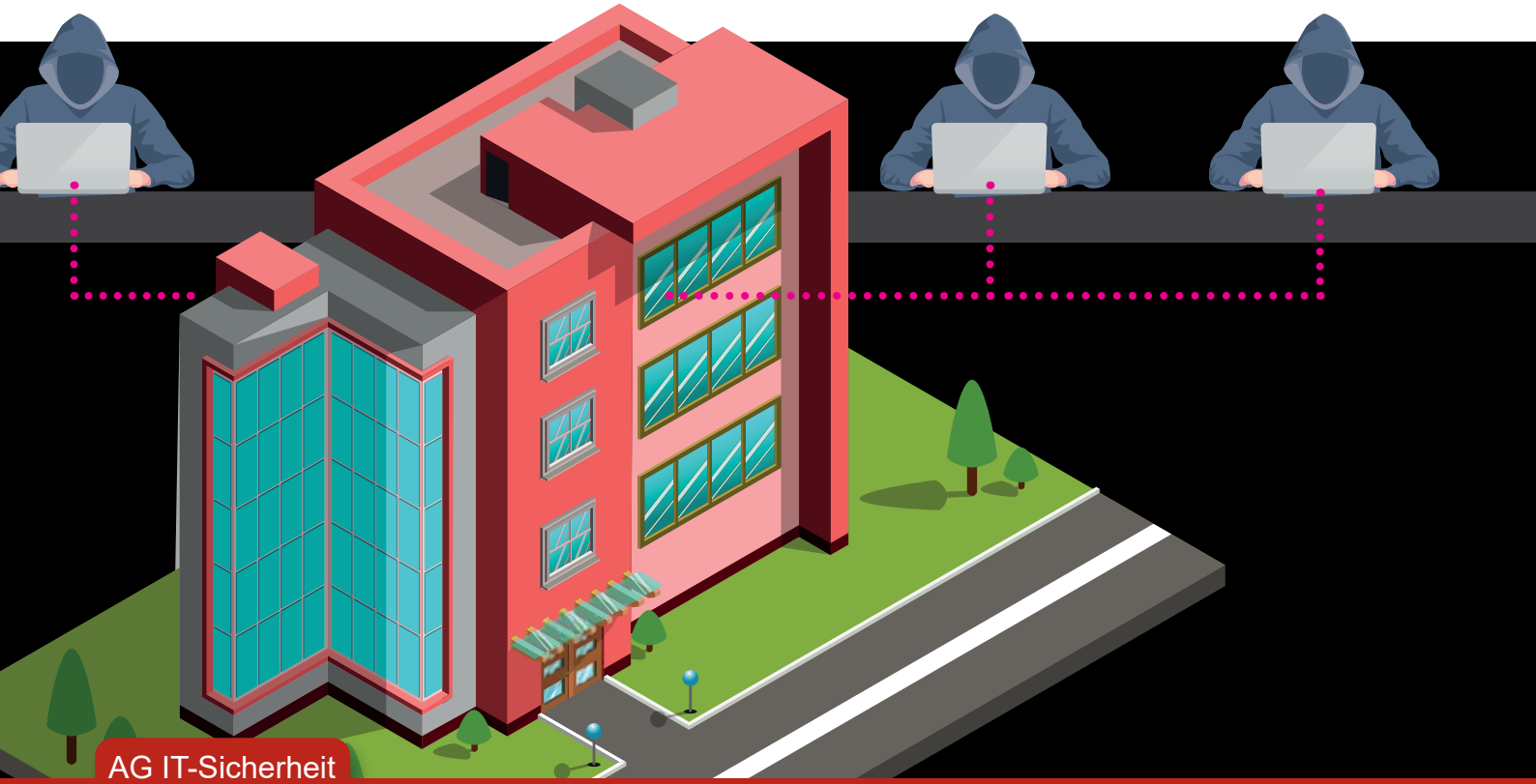
Mittelstand 4.0
Kompetenzzentren
Deutschlandweit



AG IT-Sicherheit

Gegen Cyberattacken gewappnet

Sechs Einfallstore für Cyberangriffe bei kleineren und mittleren Unternehmen

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Editorial

Liebe Leserinnen und Leser,
Fragen rund um das Thema „IT-Sicherheit“ werden immer häufiger und selbstverständlicher – auch für kleine und mittlere Unternehmen. Mit zahlreichen Förderprogrammen, einer zentralen Cybersicherheitsbehörde und einem straffen regulatorischen Rahmen ist Deutschland grundsätzlich gut aufgestellt. Nichtsdestotrotz behält die „Bedrohung aus dem Netz“ für viele kleine und mittlere Unternehmen nach wie vor einen sehr abstrakten Charakter. Vor diesem Hintergrund haben wir beschlossen, das Thema anhand von sechs fiktiven Angriffsszenarien zu konkretisieren, die auf unterschiedlichen Lagebildern zur IT-Sicherheit in Deutschland aufbauen.

„Was passiert eigentlich, wenn ich angegriffen werde?“, „Welche organisatorischen und technischen Schwachstellen werden für einen Angriff genutzt?“ und nicht zuletzt: „Was kann ich tun, wenn ich Opfer eines akuten Angriffs bin?“ Diesen und weiteren Fragen möchten wir uns in dieser Broschüre widmen.

Die Leserinnen und Leser dieser Broschüre werden durch sechs unterschiedliche Angriffsszenarien geführt, die bei mittelständischen Unternehmen in der einen oder anderen Form besonders häufig auftreten. Im Anschluss an jedes Angriffsszenario werden Definitionsmerkmale, Angriffsvektor und Hilfestellungen aufgezeigt. Bei Letzteren handelt es sich um Produkte aus dem Förderschwerpunkt „Mittelstand-Digital“ sowie aus anderen Initiativen und Einrichtungen, die wir zusammengeführt haben.

Bei der Entwicklung der Angriffsszenarien haben wir mit der Arbeitsgruppe „IT-Sicherheit“ produktiv zusammengearbeitet – dafür bedanken wir uns recht herzlich bei allen Mitgliedern der Arbeitsgruppe.

Wir hoffen, dass diese Broschüre das Thema IT-Sicherheit für Sie und Ihre Belegschaft greifbarer macht. Wir wünschen uns außerdem, dass die Broschüre Ihnen dabei hilft, sich den Herausforderungen zu stellen, die eine aktive Digitalisierung des deutschen Mittelstandes mit sich bringt.

Dr. Frauke Goll
Mittelstand 4.0-Kompetenzzentrum Stuttgart

Dr. Thomas Usländer
Mittelstand 4.0-Kompetenzzentrum Stuttgart

Inhalt

Aus der Praxis

„Heute weiß man über die Gefahren von IT-Sicherheitsvorfällen Bescheid, leitet entsprechende Maßnahmen ein und wähnt sich in Sicherheit. Bis es dann passiert …

In meiner Zeit als IT-Leiter eines mittelständischen Unternehmens hatten wir einen schweren IT-Sicherheitsvorfall durch Ransomware. Es hat Wochen gedauert, bis wir wieder in den regulären Geschäftsbetrieb gehen konnten. Alleine die Aufräumarbeiten bis hin zur Wiederaufnahme des ‚normalen' Arbeitsbetriebs haben mehrere Monate gedauert.

Vielen Geschäftsführern ist nicht klar, dass unzureichende IT-Sicherheitsmaßnahmen und ein fehlendes Krisen-Management ihr Unternehmen kosten kann und damit auch die finanzielle Lebensgrundlage vieler Mitarbeiterinnen und Mitarbeiter.

Aus meiner Erfahrung und den vielen Gesprächen, die ich seither auch mit anderen Betroffenen geführt habe, ist mein Leitsatz: ‚Für mich ist nicht die Frage, ob man Opfer eines IT-Sicherheitsvorfalls wird, sondern nur wann.' Und deshalb sollte man möglichst gut darauf vorbereitet sein."

Marcus Preschle,
Management-Berater,
ORGATEAM Unternehmensberatung GmbH

Zahlen und Fakten

Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) „zählt Ransomware [Erpressungsprogramme, siehe auch S. 9] nach wie vor zu den größten Bedrohungen für Unternehmen, Behörden und andere Institutionen sowie für Privatanwender."[1]

„Die Zahl der Schadprogramme ist auf insgesamt mehr als 900 Millionen angestiegen."[2]

„71 % aller Cyberangriffe beginnen mit Spear-Phishing-E-Mails."[3] Das sind zielgerichtete beziehungsweise personalisierte E-Mails, die die Empfängerinnen und Empfänger zu einer unbedachten und für sie schädlichen Handlung veranlassen sollen.

Deutsche Unternehmen trifft es überdurchschnittlich hart: Für sie sind die [durch Cyberattacken verursachten] **durchschnittlichen Kosten** in den vergangenen zwölf Monaten [2017] von 7,8 auf 11,1 Millionen Dollar pro Konzern **förmlich explodiert**.[4]

CEO-Fraud [Chefbetrugsmasche, siehe auch S. 13] verursachte bereits Schäden in Milliardenhöhe. Die **Tendenz** ist seit Jahren **stark steigend**.[6]

Im Jahr 2018 gaben **73 %** der befragten Unternehmen mit 100 bis 499 Mitarbeiterinnen und Mitarbeitern an, in den letzten zwei Jahren von **Datendiebstahl, Industriespionage oder Sabotage** betroffen gewesen zu sein.[5]

Neben politischen Gruppen gehören laut Bundeskriminalamt wirtschaftliche **Unternehmen** zu den **bevorzugten Zielen** von überwiegend durch sogenannte Hacktivisten[7] durchgeführtes **Website Defacement** [sichtbare „Verunstaltung" von Websites, siehe auch S. 22].

1 https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html (zuletzt aufgerufen am 20.05.20)
2 https://www.bwi.de/news-blog/blog/artikel/cyberangriffe-in-deutschland (zuletzt aufgerufen am 20.05.20)
3 https://blog.wiwo.de/look-at-it/2018/07/05/die-wichtigsten-zahlen-fakten-rund-um-cybersicherheit-im-jahr-2018 (zuletzt aufgerufen am 20.05.20)
4 https://www.finance-magazin.de/cfo/cfo-digital/kosten-fuercyberattacken-steigenrasant-2003001 (zuletzt aufgerufen am 20.05.20)
5 Nach https://de.statista.com/statistik/daten/studie/164302/umfrage/computerkriminalitaet-nach-.unternehmensgroesse-in-deutschland (zuletzt aufgerufen am 24.7.19)
6 Nach https://www.heise.de/newsticker/meldung/Social-Engineering-2-3-Milliarden-US-Dollar-Schaden-durch-CEO-Betrugsmasche-3166327.html (zuletzt aufgerufen am 20.05.20)
7 Nach HACKTIVISTEN, Bundeskriminalamt Kriminalistisches Institut Forschungs- und Beratungsstelle Cybercrime KI 16, 2016, S. 5

Icons designed von Rawpixel.com – Freepik.com

Zur Onlineversion der Broschüre:
www.mittelstand-gmbh.de

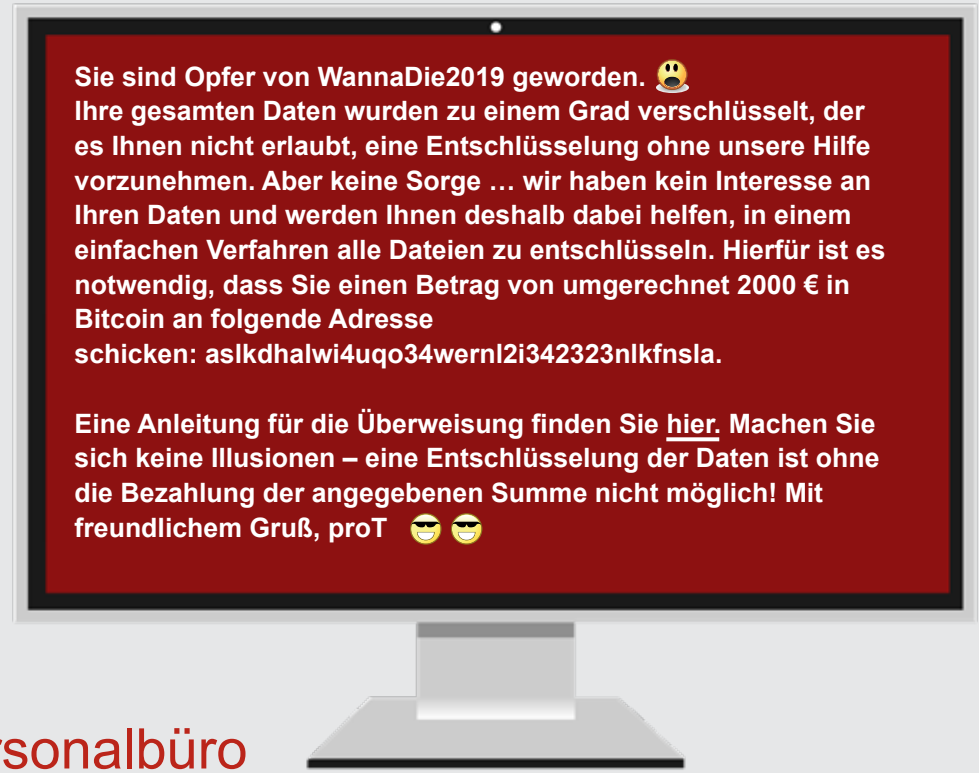
Die Mittelstand GmbH

„Die Unternehmen unterschätzen häufig, wie gravierend sich ein IT-Sicherheitsvorfall auswirken kann. Im Fall von Ransomware kann schnell der komplette Geschäftsbetrieb zum Erliegen kommen und dann wird es sehr schnell sehr teuer.“

Dr. Dirk Achenbach, Leiter der Cyberwehr Baden-Württemberg

Die Mittelstand GmbH steht stellvertretend für ein mittelständisches Unternehmen. Einzelne Abteilungen werden beispielhaft Opfer von sechs unterschiedlichen IT-Sicherheitsangriffen.

Neben der Beschreibung der Angriffe und erläuternden Texten sind zu den Angriffsszenarien viele Tipps und weiterführende Hilfestellungen samt Onlinelinks aufgeführt. Um diese Informationen einach zu nutzen, gibt es alle Texte und Links auch online unter www.mittelstand-gmbh.de.



Das Personalbüro

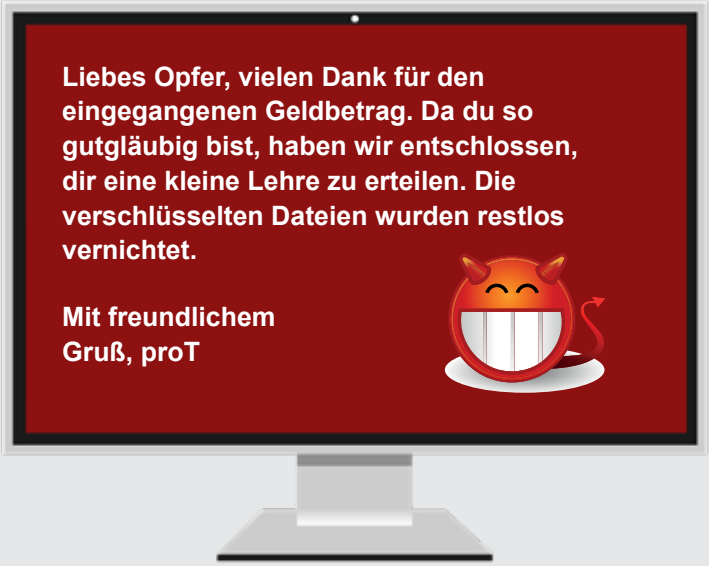
In der Mittelstand GmbH ist eine Stelle vakant. Es handelt sich dabei um den Posten der Produktionsleitung. Eines Tages erhält der zuständige Referent der Personalabteilung endlich ein Bewerbungsschreiben per E-Mail und öffnet unversehens deren Anhang.

Nach kurzer Zeit kann er nicht mehr auf die Windows-Benutzeroberfläche zugreifen. Stattdessen öffnet sich auf seinem Bildschirm ein neues Textfenster (siehe Abbildung oben).

Der Personalreferent kontaktiert umgehen die IT-Abteilung der Mittelstand GmbH und die Bereichsleiterin des Personalwesens. Es stellt sich schnell heraus, dass nicht nur lokal abgespeicherte Dateien verschlüsselt sind, sondern auch solche, die auf einem Server bearbeitet wurden. Dies betrifft alle laufenden Bewerbungsverfahren sowie die angelegten Arbeitszeitnachweise.

Gemeinsam treten die Personal- und die IT-Abteilung an die Geschäftsführung heran und teilen dieser mit,

dass die Arbeitsprozesse im Personalwesen durch eine Cyberattacke stark gestört sind. Der Leiter der IT-Abteilung muss außerdem feststellen, dass die betroffenen Dateien tatsächlich, wie vom Angreifer angedroht, verschlüsselt wurden. Entgegen der Empfehlung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) hat der Leiter der IT-Abteilung jedoch keine regelmäßigen Backups angefertigt, sodass das System nicht ohne einen Verlust der Personaldaten neu aufgesetzt werden kann.



Die Geschäftsführerin entscheidet sich gemeinsam mit dem kaufmännischen Direktor zu einem risikoreichen Schritt: Sie möchte den Betrag von 2000 € bezahlen und instruiert den IT-Beauftragten, wie in der Anleitung beschrieben vorzugehen. Nachdem der IT-Beauftragte das getan hat, erscheint ein neuer Screenlocker auf den Bildschirmen der Personalabteilung (siehe Abbildung oben).

Entstandener Schaden

- 2.000 € in Bitcoin als Zahlung an proT.
- Kosten in Höhe von mehreren Personentagen à 1.800 Euro für die Dienstleistung eines Experten für digitale Forensik sowie die „Bereinigung“ bzw. den Neuaufbau der betroffenen Server und Clients. Das Netz gilt als kompromittiert und „darf“ nicht mehr weiter vertrauensvoll genutzt werden.
- Zur Wiederherstellung der verlorenen Daten kann die Mittelstand GmbH teilweise auf eine drei Monate alte Datensicherung zurückgreifen. Alle neueren Daten müssen erneut erfasst werden.
- Der Verlust wertvoller Personal- und Bewerbungsunterlagen und damit einhergehend ein Vertrauensverlust der Mitarbeiterinnen und Mitarbeiter im Unternehmen.

Was ist passiert?
Ransomware – Erpressungsprogramme

Das englische Wort „ransom“ bedeutet in der deutschen Sprache „Lösegeld“. Der Begriff Ransomware umfasst eine Gruppe von Computerprogrammen, die den Zugriff auf Dateien oder Teile eines Computersystems einschränken beziehungsweise vorgeben dies zu tun. Der Zugang auf Dateien und Systeme wird in den meisten Fällen durch deren Verschlüsselung eingeschränkt.

Bei kleinen und mittleren Unternehmen (KMU) verfolgt der Angreifer in der Regel wirtschaftliche Interessen und erhofft sich durch seine Aktion den Erhalt des Lösegelds auf ein anonymes Konto. Das Lösegeld wird häufig in einer Kryptowährung eingefordert.

Ransomware findet häufig über das Öffnen von E-Mailanhängen, das Surfen auf infizierten Seiten („Drive-By-Exploits“) oder ein lokales Netzwerk Eingang in ein Computersystem. In manchen Fällen wird ein infizierter Anhang an möglichst viele Adressaten gesendet. Oft konzentriert sich der Angreifer jedoch auf einige wenige Unternehmen und schickt eine vermeintlich harmlose personalisierte E-Mail. Diese ist mit einer infizierten Datei versehen, sodass derjenige, der den Anhang anklickt, unfreiwillig das Einfallstor für den Angreifer öffnet. In solchen Fällen spricht man von einem personalisierten Angriff.

Ein Unternehmen, das Opfer von Ransomware geworden ist, merkt dies in der Regel schnell, da der Angreifer meist nicht lange mit seiner Forderung wartet. Oftmals öffnet sich ein Fenster in der Benutzeroberfläche des Computers. In dem Fenster wird der Geschädigte über den Angriff aufgeklärt und mit der Lösegeldforderung konfrontiert.

Wenn der Geschädigte auf die Lösegeldforderung eingeht, ist jedoch nicht sichergestellt, dass die infizierten Bereiche des Systems wieder entschlüsselt werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt deshalb im Falle eines Ransomwareangriffs den sofortigen Kontakt mit der Polizei beziehungsweise mit den dafür vorgesehenen Stellen. Es ist jedoch anzumerken, dass auch staatliche Stellen meist nicht in der Lage sind, Datenbestände zu entschlüsseln. Ist die Verschlüsselung technisch sauber umgesetzt, ist dies beim aktuellen Stand der Technik nicht möglich. Für wichtige Daten des Unternehmens (Kunden-/Projektdaten, Personaldaten, Abrechnungsdaten etc.), die für den Betrieb eines Unternehmens unabdingbar sind, emp-

fiehlt sich eine Sicherungskopie. Dann können Daten wiederhergestellt werden, ohne auf Lösegeldforderung eingehen zu müssen.

Das vom BSI generierte Lagebild für ganz Deutschland weist darauf hin, dass Ransomware nach wie vor einen maßgeblichen Teil der Internetkriminalität ausmacht. Weltweit verursachte Ransomware im analysierten Zeitraum einen Schaden von ca. 8 Milliarden US-Dollar.

Hilfestellungen

- Dass ein IT-Dienstleister Wert auf IT-Sicherheit legt, ist in der Branche leider nicht selbstverständlich. Der Leitfaden „Den richtigen IT-Dienstleister finden“[8] von gemeinsam-digital.de gibt in Form einer Checkliste Tipps zur Auswahl.
- Neben einer kurzen Einführung mit Antworten auf Fragen wie „Wie findet man heraus, ob man angegriffen wird?“ und „Wie geht man im Fall eines Angriffs vor?“ bietet der Flyer „Was tun bei einem Sicherheitsvorfall?“ auch „10 Goldene Regeln für den Umgang mit einem Sicherheitsvorfall“[9].
- Bundesamt für Sicherheit in der Informationstechnik (BSI) mit Empfehlungen zu Datensicherung und Speichermethoden[10] .
- SiBa-App – Sicherheitsbarometer mit aktuellen Warnmeldungen und Tipps fürs Handy[11].
- Deutschland sicher im Netz (DsiN): Video über Ransomware und IT-Sicherheit im Allgemeinen[12].

„IT-Sicherheit muss nicht in jedem Fall in einer großangelegten unternehmensweiten Strategie umgesetzt werden. Die Hauptsache ist zunächst, dass man in einem kontinuierlichen Prozess auch mal an Teilaspekten der Sicherheit arbeitet. So ist es leichter, die Mitarbeiter einzubinden und im Arbeitsalltag ein Bewusstsein für Sicherheitsthemen zu schaffen.“
Nico Vitt, Mittelstand 4.0-Kompetenzzentrum Siegen

8 https://gemeinsam-digital.de/app/uploads/2018/04/check-06-den-richtigen-it-dienstleister-finden-web.pdf (zuletzt aufgerufen am 20.05.20)
9 http://www.prozesse-mittelstand.digital/images/PDF/Flyer_Sicherheitsvorfall.pdf (zuletzt aufgerufen am 20.05.20)
10 https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Datensicherung/datensicherung_node.html (zuletzt aufgerufen am 20.05.20)
11 https://www.sicher-im-netz.de/node/1648 (zuletzt aufgerufen am 20.05.20)
12 https://www.youtube.com/watch?v=YueZ6kv8TSA (zuletzt aufgerufen am 20.05.20)

Die Geschäftsführung

Die Mittelstand GmbH macht jährlich 3,2 Mio. € Umsatz. In einer wöchentlichen Sitzung erläutert der Finanzdirektor des Unternehmens vor der gesamten Geschäftsführung die Entwicklung aller Ein- und Ausgänge der Unternehmensfinanzen sowie den Investitionsplan für das laufende und das kommende Quartal.

Während der Finanzdirektor die Zahlungsausgänge in einer grafischen Darstellung präsentiert, richtet sich die Aufmerksamkeit der Geschäftsführerin auf eine Einzelüberweisung von 75.000 €, die sie nicht zuordnen kann. Auf Nachfrage der Geschäftsführerin kommt der Finanzdirektor ins Schwitzen, denn auch er kann den Zahlungsausgang nicht zuordnen. Die Sitzung wird unterbrochen und der Finanzdirektor begibt sich in die Buchhaltung, wo er einen Sachbearbeiter bittet den Vorgang zu prüfen.

„Das Thema IT-Sicherheit ist auch für KMU zunehmend präsent. Die stetig wachsende Zahl von Vorfällen zwingt KMU zum Handeln. Hierbei liegt der Fokus oft auf technischen Schutzmaßnahmen. Der Aspekt der organisatorischen Schutzmaßnahmen kommt hingegen oft zu kurz.“
Christopher Tebbe, Mittelstand 4.0-Kompetenzzentrum Hannover

Es stellt sich heraus, dass der Betrag auf ein Konto in den Drittstaat Gibraltar überwiesen wurde. Der Sachbearbeiter erklärt, dass er per Mail eine Rechnung erhalten habe, auf der die Summe von 75.000 € mit der Bitte um sofortige Überweisung angegeben ist. Außerdem hat der Sachbearbeiter parallel zum Eingang der Rechnung eine E-Mail aus dem Büro der Geschäftsführerin erhalten, die ebenfalls auf eine umgehende Überweisung des Betrags dringt. Als Grund für die Dringlichkeit gibt das Büro der Geschäftsleitung das Risiko eines ver-

„Aus der praktischen Erfahrung und aus wirtschaftlicher Sicht empfiehlt sich eine angemessene, gleichmäßige Bearbeitung aller Anforderungen an die IT-Sicherheit. Die Mitarbeiter sind ein Schlüsselfaktor und müssen die technischen und organisatorischen Rahmenbedingungen sowie die daraus resultierenden Prozesse kennen, verstehen und anwenden. Daher ist es dringend zu empfehlen, bei den Mitarbeiterinnen und Mitarbeitern ein Bewusstsein und eine Sensibilisierung in Hinblick auf das Thema IT-Sicherheit zu schaffen.“

Sabine Betzholz-Schlüter,
Mittelstand 4.0 Kompetenzzentrum Saarbrücken

zögerten Eingangs der Ware und einen damit verbundenen Produktionsausfall an. In der E-Mail ist für den Fall der verzögerten Produktion ein Verlust von mindestens 500.000 € angegeben. Da der Finanzdirektor an diesem Tag im Urlaub war, gab es keine Möglichkeit für Rückfragen.

Der Finanzdirektor lässt sich den E-Mailverkehr ausdrucken und wendet sich direkt an die Geschäftsführerin. Die Assistentin der Geschäftsführung, die laut E-Mailverkehr die Nachricht geschickt hat, sowie die Geschäftsführerin selbst beteuern, dass sie von dem Vorgang nichts wissen.

Nachdem nun auch der Leiter der IT-Abteilung hinzugezogen wurde, wird klar, dass die E-Mail zwar vom E-Mail-Konto der Assistentin verschickt, jedoch nicht von ihr verfasst wurde. Offenbar hat es einen Zugriff von einer unbekannten IP-Adresse gegeben.

Es stellt sich heraus, dass sich der Angreifer über eine Schwachstelle im System Zugang zur gesamten Unternehmenskommunikation verschafft hat. So war es möglich den Kalender des Finanzdirektors einzusehen und eine Nachricht vom E-Mail-Account der Geschäftsführungsassistenz zu schreiben. Obwohl der Finanzdirektor den Vorgang zur Anzeige bringt, können die deutschen Behörden nichts für ihn tun, da sich das Konto des Angreifers in einem Drittstaat befindet und dort anonym geführt wird.

Entstandener Schaden

- 75.000 Euro.

Was ist passiert?
CEO-Fraud – Chefbetrugsmasche

Der Begriff „CEO-Fraud“ setzt sich aus den beiden englischen Wörtern für „Geschäftsführer“ und „Betrug“ zusammen. Bei CEO-Fraud handelt es sich um eine „Social-Engineering“-Strategie. Unter „Social Engineering“ (frei übersetzt: „soziale Manipulation“) versteht man die Beeinflussung von Menschen, um sie dazu zu bringen, bestimmte Dinge zu tun, beispielsweise ein Geheimnis preiszugeben.

Beim CEO-Fraud gibt sich der Angreifer als Geschäftsführer, leitender Angestellter oder Rechtsbeistand eines Unternehmens aus und baut Kontakt zu einem oder mehreren Angestellten eines Unternehmens (oftmals in der Buchhaltung oder dem Rechnungswesen) auf. Er gibt vor, selbst der Geschäftsführer zu sein oder entsprechende Vollmachten zu besitzen. Der Mitarbeiter des betroffenen Unternehmens wird per E-Mail oder Telefon dringend dazu aufgefordert, einen Geldbetrag auf das vermeintliche Konto eines Geschäftspartners zu überweisen. Oftmals werden Gründe wie „Zahlungsverzug“ oder „strikte Geheimhaltung“ angeführt, um den Mitarbeiter des Unternehmens dazu zu bewegen, keine Rücksprache mit anderen Stellen zu halten. CEO-Fraud lebt von der Affekthandlung des Mitarbeiters im Unternehmen.

Die Angriffe werden meistens gut vorbereitet. Im Vorfeld werden das Kommunikationsverhalten bestimmter Mitarbeiterinnen und Mitarbeiter sowie ihre Kompetenzen im Unternehmen ausgespäht. Dies geschieht in vielen Fällen über Social Media Plattformen wie XING, LinkedIn, Facebook, Twitter etc., auf denen sie bewusst Informationen zu sich und ihrer Rolle im Unternehmen preisgeben.

Die Motivation des Angreifers ist in der Regel wirtschaftlicher Natur. Das betroffene Unternehmen muss damit rechnen, dass der ökonomische Schaden nicht wieder rückgängig gemacht werden kann. Für CEO-Fraud werden in vielen Fällen bewusst Konten genutzt, die sich in Ländern befinden, die ein Eingreifen der Behörden nahezu unmöglich machen.

Im aktuellen Lagebericht zur IT-Sicherheit in Deutschland warnt das Bundesamt für Sicherheit in der Informationstechnik (BSI) explizit vor CEO-Fraud. Das Bundeskriminalamt (BKA) schätzt den jährlichen Schaden für Deutschland auf einen zweistelligen Millionenbetrag. Das Federal Bureau of Investigation

(FBI) geht sogar von einem weltweiten Schaden von 3,1 Mrd. US-Dollar aus.

Das BSI empfiehlt geschädigten Unternehmen in jedem Fall Strafanzeige bei der örtlichen Polizeistelle zu erstatten. Eine unterlassene Strafanzeige aus „falscher Scham“ schützt nur die Täter.

Hilfestellungen

- SiToM[13] (Sicherheitstool Mittelstand): kostenloses Werkzeug, um sich einen schnellen Überblick über den Status der IT-Sicherheit im eigenen Unternehmen zu verschaffen.
- DsiN – Sicherheitscheck[14] von sicher-im-netz.de: sehr ähnlich zu SiToM.
- Vier-Augen-Prinzip: Insbesondere beim Bewegen großer Geldbeträge, wie es in Unternehmen häufig vorkommt, kann es sinnvoll sein, das Vier-Augen-Prinzip einzuführen. Das Vier-Augen-Prinzip hat als Ziel, das Risiko für Fehler und Missbrauch zu verringern, indem Entscheidungen von zwei Personen parallel und unabhängig voneinander getroffen werden. Nur wenn beide dieselbe Entscheidung treffen, wird die entsprechende Aktion durchgeführt. Dazu ist es vor allem wichtig, dass die eingesetzten Personen voneinander persönlich und organisatorisch unabhängig sind, da es sonst zu Interessenskonflikten kommen kann.
- Leitfaden für Mitarbeiterinnen und Mitarbeiter mit Verhaltensregeln zum Thema „Social Engineering“[15] von sicher-im-netz.de.

„Kleine und mittlere Unternehmen müssen in die Lage versetzt werden, Sicherheitsrisiken in einem gewissen Umfang selbst identifizieren und evaluieren zu können. In einem nächsten Schritt können sie dann gemeinsam mit einem Dienstleister entscheiden, ob sie den Mehraufwand für die zu implementierenden Maßnahmen tragen oder lieber den risikobasierten Ansatz wählen möchten.“
David Ruge, Mittelstand 4.0 Kompetenzzentrum Stuttgart

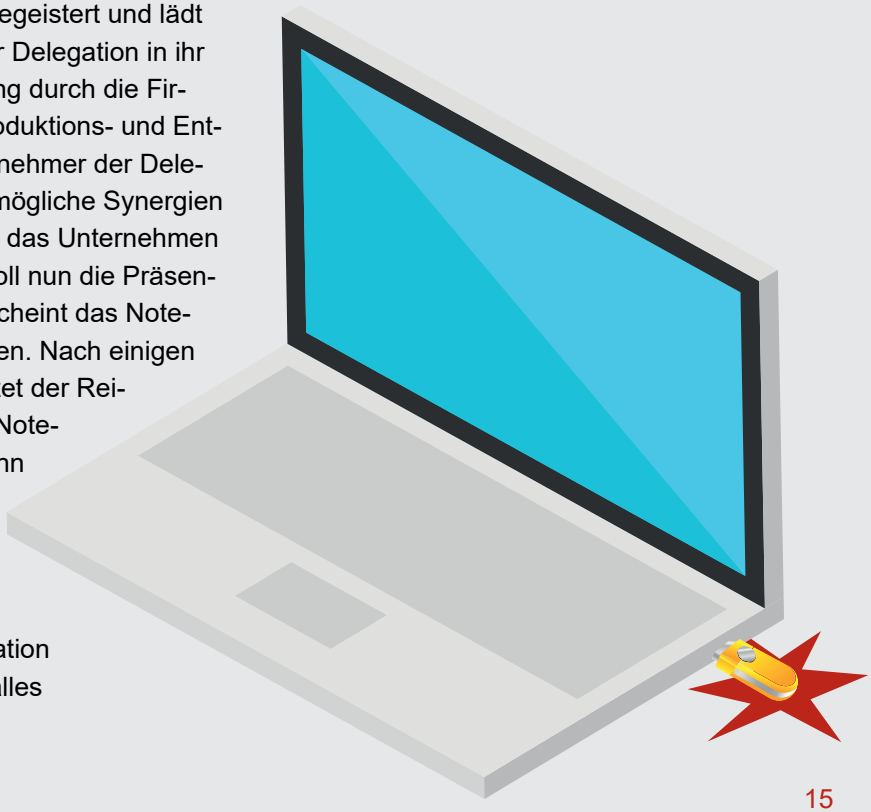
13 https://www.sitom.de/home (zuletzt aufgerufen am 20.05.20)
14 https://www.sicher-im-netz.de/dsin-sicherheitscheck (zuletzt aufgerufen am 20.05.20)
15 https://www.sicher-im-netz.de/sites/default/files/download/leitfaden_social_engineering.pdf (zuletzt aufgerufen am 20.05.20)

Die Entwicklungsabteilung

Die Entwicklerinnen und Entwickler der Mittelstand GmbH sind der ganze Stolz des Unternehmens. Sie haben ihren Finger stets am Puls der Zeit und entwickeln das Portfolio ihres Arbeitsgebers laufend weiter. In der örtlichen Industrie- und Handelskammer (IHK) bezeichnet man die Mittelstand GmbH deshalb sogar als „hidden champion“ ihres Marktsegments.

„Mit der digitalen Durchdringung aller Gesellschafts- und Wirtschaftsbereiche steigen die Anforderungen an die IT-Sicherheit.“
Falk Witzel, Deutsches Zentrum für Luft- und Raumfahrt

Um die Mittelstand GmbH auch international stärker zu vernetzen, bietet die IHK dem Unternehmen an, Teil eines Netzwerks zu werden, bei dem sich regelmäßig diverse in- und ausländische Marktteilnehmer präsentieren. Die Geschäftsführerin der Mittelstand GmbH ist sofort begeistert und lädt die Teilnehmerinnen und Teilnehmer einer Delegation in ihr Unternehmen ein. Geplant ist eine Führung durch die Firmenräume und ein kurzer Blick in das Produktions- und Entwicklungslabor. Im Gegenzug soll ein Teilnehmer der Delegation sein Unternehmen vorstellen, um mögliche Synergien zu identifizieren. Nach der Führung durch das Unternehmen und einem ausgelassenen Mittagessen soll nun die Präsentation der Delegation stattfinden. Leider scheint das Notebook des Reiseleiters nicht zu funktionieren. Nach einigen Minuten des vergeblichen Probierens bietet der Reiseleiter an, seine Präsentation an einem Notebook der Mittelstand GmbH zu halten, denn er hat glücklicherweise die Präsentation auf einem USB-Stick gesichert. Die Geschäftsführerin weist ihre Assistentin an, dem seriösen Reiseleiter ein Firmennotebook für die Präsentation zur Verfügung zu stellen. Es funktioniert alles



„Wertvolles Know-how und Unternehmensdaten sind ein attraktives Ziel für Industriespionage. Besonders problematisch dabei ist, dass hier mitunter staatliche Akteure beteiligt sein können, die über fortschrittliche Angriffstechniken, Zeit und Ressourcen verfügen. Das rechtzeitige Erkennen und die Abwehr dieser Advanced Persistent Threats (APT) erfordern umfassende Sicherheitsvorkehrungen.“

Christoph Frohneberg, Disponent Cyberwehr Baden-Württemberg

einwandfrei und der Reiseleiter kann seinen Zuhörerinnen und Zuhörern von seinem Unternehmen berichten, das ein ähnliches Produktportfolio wie die Mittelstand GmbH besitzt. Die Geschäftsführerin stellt sich bereits eine enge Kooperation mit dem Unternehmen vor.

Nach einigen Monaten versucht die Geschäftsführerin der Mittelstand GmbH vergeblich Kontakt mit dem Leiter der Unternehmensdelegation aufzunehmen. Da die Geschäftsführerin jedoch unbedingt auf dem Heimatmarkt des Partners in spe expandieren will, beschließt sie schon vor dem Abschluss der Kooperation ein Patent für das Kernprodukt der Mittelstand GmbH bei den Behörden des Landes anzumelden. Mit großem Schrecken muss sie jedoch feststellen, dass vor einigen Monaten bereits ein solches Patent angemeldet wurde. Der Eigentümer des Patents ist das Unternehmen, das noch vor kurzem im Rahmen der Delegationsreise bei der Mittelstand GmbH zu Besuch war. Ein Vertrieb des Produkts auf dem angestrebten Markt ist also nicht möglich.

Nach langem Überlegen und mehreren Krisensitzungen stellt sich heraus, dass ein Firmennotebook über einen USB-Stick infiziert wurde und sich ein externer Akteur so Zugriff auf das Firmennetzwerk verschafft hat. Neben dem gesamten E-Mail-Traffic wurden auch Konstruktionspläne und Skizzen aus der Entwicklungsabteilung abgegriffen.

Entstandener Schaden

- Verlust des Patents und daraus folgend der Verlust eines neuen Absatzmarktes.

Was ist passiert?
Datendiebstahl via Malware

Als „Malware“ werden Programme bezeichnet, die auf einem Computersystem schädliche Funktionen auslösen oder steuern. Der Datendiebstahl (englisch „Data Breach“) bezeichnet einen Vorgang, bei dem geschützte Daten einer Organisation oder einer Privatperson ohne deren Zustimmung entwendet werden.

Neben Social-Engineering-Strategien ist Malware ein beliebter Weg, um sich Zugang zu Systemen und den darauf abgelegten Daten zu verschaffen. Laut Cyber-Sicherheits-Umfrage von 2017 der Allianz für Cyber-Sicherheit sind Malware-Infektionen bei Unternehmen erneut die häufigste Angriffsart.

Computersysteme werden oftmals durch Dateianhänge in E-Mails, durch externe Geräte wie USB-Sticks oder schlecht gesicherte Fernzugänge (VPN, RDP etc.) infiziert. Der Geschädigte merkt in der Regel nicht, dass er Opfer einer Malwareattacke wurde. Der Datenabfluss ist für den einfachen Nutzer unsichtbar. Neben PC-Systemen geraten auch Smartphones immer öfter ins Visier von Angreifern, da auch sie wertvolle Daten enthalten, die Aufschluss zu Vorgängen in Unternehmen geben können.

Im aktuellen Lagebericht zur IT-Sicherheit in Deutschland weist das Bundesamt für Sicherheit in der Informationstechnik (BSI) darauf hin, dass zusätzlich zu den Schadprogrammen für PC innerhalb des Berichtszeitraums pro Monat durchschnittlich etwa 690.000 neue Schadprogramme für das Mobilbetriebssystem Android beobachtet wurden. Die Behörde erwartete zu diesem Zeitpunkt einen Anstieg der Schadprogramme für Androidsysteme auf 30.000.000 allein für das Jahr 2018.

Das Ziel des Angreifers ist in diesem Szenario wirtschaftlicher oder politischer Natur. Ein politisches Motiv spielt dann eine Rolle, wenn Unternehmen und Organisationen eine strategische Bedeutung (kritische Infrastrukturen, spezielle Dienstleister und Zulieferer, Rüstungsindustrie etc.) beigemessen wird. Ein wirtschaftliches Motiv spielt in der Regel dann eine Rolle, wenn der Angreifer erbeutete Daten veräußern oder für eigene Zwecke nutzen möchte.
Es werden immer häufiger Fälle bekannt, in denen Datenhandel zwischen Hackern und Personen betrieben wird, die in Konkurrenz zu einem Unternehmen stehen und diesem einen Reputationsschaden zufügen wollen. Auch ein direkter ökonomischer Schaden kann durch den Datenhandel erzielt werden, wenn

„Insbesondere im industriellen Umfeld empfiehlt sich eine ganzheitliche Betrachtung der IT-Sicherheit. Diese umfasst Organisation, Prozesse, Technologie und Mensch. Dazu gehört auch die Berücksichtigung der Wertschöpfungskette vom Hersteller über den Integrator bis hin zum Betreiber. Der empfohlene Ansatz findet sich unter anderem in der Norm IEC 62443 wieder.“

Sabine Betzholz-Schlüter,
Mittelstand 4.0 Kompetenzzentrum Saarbrücken

Kundendaten abhandenkommen und somit ein betriebliches Kontinuitätsmanagement oft unmöglich wird.

Hilfestellungen

- Leitfaden mit Verhaltensregeln zum Thema „Social Engineering“[16] von sicher-im-netz.de zur Sensibilisierung von Mitarbeiterinnen und Mitarbeitern für Angriffe, insbesondere hinsichtlich Social Engineering.
- Das Bundesamt für Sicherheit in der Informationstechnik (BSI) über die Risiken von Schadprogramme[17].
- Video über Ransomware und IT-Sicherheit im Allgemeinen[18] von Deutschland sicher im Netz (DsiN).

16 https://www.sicher-im-netz.de/sites/default/files/download/leitfaden_social_engineering.pdf (zuletzt aufgerufen am 20.05.20)
17 https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/Schadprogramme/schadprogramme_node.html (zuletzt aufgerufen am 20.05.20)
18 https://www.youtube.com/watch?v=YueZ6kv8TSA (zuletzt aufgerufen am 20.05.20)

Die Kommunikationsabteilung

Frau Müller-Lüdenscheidt ist Referentin in der Kommunikationsabteilung der Mittelstand GmbH. Sie ist insbesondere für die Pressearbeit sowie für sämtliche Kanäle der externen Kommunikation verantwortlich. Zu letzteren gehören die Website des Unternehmens und alle Social-Media-Kanäle. Obwohl die Mittelstand GmbH ein Unternehmen mittlerer Größe ist, legt die Geschäftsführung besonders viel Wert auf die Außenwirkung des Unternehmens. Das hat damit zu tun, dass ein Großteil der Kunden online akquiriert wird. Außerdem betreibt das Unternehmen eine Bestellplattform, die ca. 80 % des gesamten Bestellaufkommens bedient.

Als Frau Müller-Lüdenscheidt an einem Montagmorgen wie immer als Erste ins Büro kommt und die Website der Mittelstand GmbH aufruft, fällt sie fast vom Stuhl. Anstelle der modernen und ansprechenden Unternehmenswebsite findet sie folgendes Textfenster vor:

„Ein zunehmender Digitalisierungsgrad erhöht gleichzeitig die Anforderungen an die Systemverantwortlichen. Verwendete Komponenten müssen regelmäßig auf Updates überprüft und gegebenenfalls aktualisiert werden.“
Sven Mattheis, Mittelstand 4.0-Kompetenzzentrum Bremen

Frau Müller-Lüdenscheidt ruft umgehend ihre Vorgesetzte an und berichtet ihr von der gehackten Website. Nachdem die Nachricht die Geschäftsführung erreicht hat, wird ein Krisenstab eingerichtet, um das Problem zu lösen. Die Agentur, die für die äußere Erscheinung der Website zuständig ist, wird ebenfalls hinzugezogen.

In enger Zusammenarbeit zwischen Agentur und IT-Abteilung der Mittelstand GmbH wird schließlich festgestellt, dass lediglich der sichtbare Teil der Website von dem Angriff betroffen ist. Die eigentliche Logik, die im Hintergrund die Bestellungen abwickelt, läuft auf den firmeneigenen Servern der Mittelstand GmbH und blieb bei der Attacke unberührt. Eine Einschränkung der Funktionen der Bestellplattform oder ein Datenabfluss kann also, entgegen der Nachricht des Angreifers, nicht festgestellt werden.

Als Einfallstor diente dem Angreifer die nicht aktualisierte Version des Content-Management-Systems, das die Agentur verwendet, um die Website zu verwalten. Der Leiter der IT-Abteilung analysiert die Aktivitäten des Webservers und muss feststellen, dass die Website bereits in der Nacht von Freitag auf Samstag gehackt wurde. Das Fenster mit der Nachricht des Angreifers ist also schon über das gesamte Wochenende sichtbar.

Nachdem die Geschäftsführerin die örtliche Anlaufstelle für Cybercrime bei der Polizei kontaktiert hat, stellt sich heraus, dass die Mittelstand GmbH nicht die einzige Geschädigte ist. In dem Marktsegment wurden im Laufe des Wochenendes diverse Websites gehackt. Eine Ausnahme bildet dabei ein größeres Unternehmen, welches den Markt dank einer aggressiven Marketingstrategie seit einiger Zeit dominiert.

Die Geschäftsführerin muss im Nachgang feststellen, dass der Vorfall auf der Kundenseite zu einem massiven Vertrauensverlust geführt hat. Obwohl ein Abfluss von Kundendaten nicht stattgefunden hat und die Kommunikationsabteilung dies in mehreren Pressemitteilungen immer wieder betont, sind die Bestellungen stark zurückgegangen. Parallel dazu kämpft die Kommunikationsabteilung mit einer Flut von Nutzeranfragen bzgl. der angeblich weitergeleiteten Daten.

Auch für die Agentur, die die Website verwaltet, hat der Vorfall Konsequenzen: Nachdem die Firmenleitung der Mittelstand GmbH erfährt, dass der Angriff nur aufgrund der unterlassenen Softwareaktualisierung durchgeführt werden konnte, kündigt sie das Geschäftsverhältnis mit dieser Agentur auf und begibt sich auf die Suche nach einem Dienstleister, der mehr Wert auf IT-Sicherheit legt.

Entstandener Schaden

- Umsatzeinbußen durch den zweitägigen Ausfall der Bestellplattform.
- Erhöhter Arbeitsaufwand zur Bearbeitung von Anfragen besorgter Kundinnen und Kunden.
- Das Vertrauensverhältnis zwischen Kundinnen und Kunden und Unternehmen wurde nachhaltig gestört.

„Präventionsmaßnahmen sollen IT-Sicherheitsvorfälle verhindern. Man muss sich aber zusätzlich einen Plan zurechtlegen, wie man im Notfall vorgeht.“

Dirk Achenbach, Leiter der Cyberwehr Baden-Württemberg

Was ist passiert? Manipulation von Websites am Beispiel des Website Defacements

Das englische Wort „defacement“ bedeutet in der deutschen Sprache „Verunstaltung“. Bei Website Defacement handelt es sich um die Veränderung von sichtbaren Inhalten auf Internetseiten durch Dritte. Der Vorgang wird oft als das digitale Pendant zum Vandalismus der analogen Welt bezeichnet.

Die Beweggründe für die Manipulation von Websites sind mannigfaltig. Manche Angriffe sollen unbemerkt bleiben. Dann baut der Angreifer zum Beispiel seine Schadsoftware so in die Website ein, dass möglichst viele Websitebesucher diese unwissentlich herunterladen und sich somit infizieren.

Einige Angreifer übernehmen auch Webserver, um diese dann unbemerkt als „Kommandozentrale“ zu nutzen. Wenn der Angreifer beispielsweise eine größere Zahl an Rechnern gekapert hat, die für ihn arbeiten (man spricht dann von Bots), kann er diese so konfigurieren, dass sie in regelmäßigen Abständen bei der übernommenen Website (der „Kommandozentrale“) vorbeikommen, um sich neue Befehle oder Updates für die von ihnen ausgeführte Schadsoftware abzuholen. Dies hat für den Angreifer den großen Vorteil, dass der Angriff nicht so leicht auf ihn zurückgeführt werden kann.

Ein anderes, relativ neues Vorgehen stützt sich auf den guten Ruf, den manche Websites sich über Jahre hinweg aufgebaut haben. Der Angreifer übernimmt die Website und baut auf einer Unterseite einen Fake-Shop oder Werbung für einen solchen ein. Den Rest der Website lässt er intakt. Die Suchmaschinen, die die ursprüngliche, unveränderte Seite als seriös bewerteten, geben dem Fake-Shop auf der Unterseite nun ebenfalls eine seriöse Bewertung, was letztlich für mehr Verkäufe in diesem Shop sorgt. Das spült wiederum Geld in die Kasse des Angreifers.

Eine weitere Art von Angriffen ist absichtlich so gestaltet, dass sie nach außen sichtbar ist. Dies geschieht zum Beispiel, um ein Exempel zu statuieren oder dem verantwortlichen Hacker in der Szene Ansehen zu verschaffen. Dazu gehört auch das sogenannte Website Defacement.

Für die Veränderung von optischen Inhalten auf Internetseiten werden in vielen Fällen Schwächen des Content-Management-Systems (CMS) genutzt. Das CMS ist eine Plattform, auf der unterschiedliche Programme zur Bearbeitung von Website-Inhalten zusammenlaufen. Gängige Plattformen sind WordPress, TYPO3 und Joomla. Neben der Nutzung von Schwachstellen im CMS sind beim Website Defacement auch Social-Engineering-Strategien sehr beliebt (siehe S. 13).

Der Angreifer ist entweder politisch oder wirtschaftlich motiviert. Es sind diverse Fälle bekannt, in denen das Website Defacement als Instrument zur Schädigung von Konkurrenz genutzt wurde – etwa zur Generierung von negativer Öffentlichkeit oder zur Verbreitung von Fehlinformationen. In manchen Fällen wird Website Defacement auch zur Erpressung eines Lösegelds genutzt. Insbesondere Webshops und Buchungsplattformen können durch Website Defacement großen Schaden erleiden, da eine „verunstalte“ Seite sehr große Auswirkungen auf das Kundenverhalten, die wahrgenommene Glaubwürdigkeit und letztendlich auch auf den Umsatz eines Unternehmens haben kann.

Das Unternehmen muss je nach Frequenz der eigenen Internetpräsenz damit rechnen, dass ein Teil der Kunden und Geschäftspartner den Angriff wahrnehmen. Um den Schaden zu beheben, muss das Unternehmen Ressourcen mobilisieren, um den eigenen Internetauftritt sowie die positive öffentliche Wahrnehmung wiederherzustellen. Ersteres ist in der Regel ohne größeren Aufwand möglich, sofern die Inhalte der Internetseite gesichert wurden (viele CMS bieten solche Funktionen an). Die Wiederherstellung der öffentlichen Wahrnehmung ist in vielen Fällen schwieriger und hängt vom Umfang des Angriffs sowie dem Geschick der Kommunikationsabteilung ab.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt im Falle eines Website Defacements grundsätzlich auch die

„Website Defacement ermöglicht es ideologisch motivierten Personen, sich die Reichweite einer fremden Internetpräsenz zu Nutze zu machen, um den Ruf des Unternehmens zu schädigen.“

Christoph Frohneberg, Disponent Cyberwehr Baden-Württemberg

„Website Defacements sind mehr als digitales Graffiti an der Firmenzentrale. Gut getimed können sie – beispielsweise durch Fehlinformationen – Aktienkurse einbrechen lassen.“

Christoph Frohneberg, Disponent Cyberwehr Baden-Württemberg

Unternehmensleitung sowie die Pressestelle bzw. die für Öffentlichkeitsarbeit zuständige Organisationseinheit zu informieren.

Hilfestellungen

- SIWECOS[19] (Abkürzung für: Sichere Webseiten und Content Management Systeme): kostenloses Werkzeug zum Überprüfen, ob eine Website bzw. das hinter der Website arbeitende Content Management System über bekannte Schwachstellen verfügt.
- SiToM[20] (Abkürzung für: Sicherheitstool Mittelstand): kostenloses Werkzeug, um sich einen schnellen Überblick über den Status der IT-Sicherheit im eigenen Unternehmen zu verschaffen.
- DsiN-Sicherheitscheck[21]: ein leichter Einstieg zur Ermittlung des IT-Sicherheitsniveaus in kleinen und mittleren Unternehmen (KMU) mit Handlungsempfehlungen (ähnlich wie SiToM).
- „10 Punkte für einen sicheren Umgang mit Unternehmensdaten im Internet“[22], herausgegeben vom Bundesministerium für Wirtschaft und Energie.

19 https://siwecos.de (zuletzt aufgerufen am 20.05.20)
20 https://www.sitom.de (zuletzt aufgerufen am 20.05.20)
21 https://www.sicher-im-netz.de/dsin-sicherheitscheck (zuletzt aufgerufen am 20.05.20)
22 https://www.bmwi.de/Redaktion/DE/Downloads/0-9/10-punkte-fuer-einen-sicheren-umgang-mit-unternehmensdaten-im-internet.pdf?__blob=publicationFile&v=3 (zuletzt aufgerufen am 20.05.20)

Die Lieferkette

Der Automobilindustrie geht es gut in Deutschland. Und so auch der Mittelstand GmbH, denn als Automobilzulieferer konnte sich das Familienunternehmen in den letztenJahrzehnten mit seinen ausgeklügelten Fertigungsmethoden eine starke Stellung im Markt sichern.

Um diese Markstellung zu wahren und zu festigen, setzt das Unternehmen seit seiner Gründung auf ein Zusammenspiel aus dem strengen Schutz der Firmengeheimnisse, der Patentsicherung und der Bindung der angestellten Fachkräfte. Seit die Digitalisierung Einzug in das Unternehmen gehalten hat, wird auch ein großes Augenmerk auf die IT-Sicherheit gelegt und das Personal umfassend geschult.

Doch auf den Besuch, den die Geschäftsführung eines Mittwochs erhält, kann trotzdem niemand gefasst sein: Das Bundeskriminalamt (BKA) steht mit einer ganzen Mannschaft vor der Tür und fordert die Mittelstand GmbH zur Mitarbeit in einem der Geheimhaltung unterliegenden Fall auf. Bei Nichtkooperation würde stattdessen die Durchsuchung sämtlicher Firmengebäude und die Beschlagnahmung der gesamten IT-Infrastruktur erfolgen. Der Grund: Verdacht auf Wirtschaftsspionage und Computerkriminalität.

Selbstverständlich willigt die Firmenleitung in die Kooperation mit dem BKA ein, nicht zuletzt, weil sonst ein Totalausfall der Produktion bevorstehen würde. Ab diesem Zeitpunkt sind täglich Computerspezialisten des BKA und des Bundesamts für Sicherheit in der Informationstechnik (BSI) in der Firma. Die Firmenleitung wird gebeten, ihnen für ihre Arbeit eigene Räumlichkeiten zur Verfügung zu stellen.

In den folgenden Monaten kommt der Flurfunk nicht mehr zur Ruhe. Inzwischen hat man sich sogar mit den schweigsamen Gästen vom BKA

„Den Wettlauf zwischen Angreifer und Sicherheitsabteilung kann die Sicherheitsabteilung nicht gewinnen ... sie muss ihn aber auch nicht verlieren.“
Sven Mattheis, Mittelstand 4.0-Kompetenzzentrum Bremen

mit der großen Vorliebe für Mate-Tee-haltige Erfrischungsgetränke arrangiert, aber was wirklich los ist, weiß immer noch nur ein sehr kleiner Kreis von Eingeweihten.

Erst als die Ermittlungen abgeschlossen sind, gibt die Geschäftsleitung in einem firmeninternen Schreiben Details zu den Vorkommnissen bekannt:

Vor zwei Jahren wurden bei der Mittelstand GmbH in allen Abteilungen neue Festnetztelefone eingeführt. Der Funktionsumfang dieser Geräte ist so groß, dass die Lektüre der Betriebsanleitung mehrere lange Nachmittage und viele Tassen Kaffee beanspruchen würde. Wie sich herausstellt, haben die Angreifer die Software, die auf diesen Telefongeräten läuft, auf eine Weise manipuliert, dass die Telefongeräte in erster Linie für die Angreifer arbeiteten, Informationen an diese weiterleiteten und von ihnen Befehle entgegennahmen.

Mithilfe der so gewonnen Informationen war es den Angreifern ein Leichtes, nach und nach mittels gefälschter Mails und ausgenutzter Sicherheitslücken bis in die Computer der Geschäftsleitung vorzudringen. All diese Vorgänge wurden weder von der IT-Abteilung noch von anderen Mitarbeiterinnen und Mitarbeitern des Betriebs bemerkt.

Die Mittelstand GmbH selbst war jedoch nur eine Zwischenstation bei dem mit großer Expertise ausgeführten Angriff. Eigentlich hatten die Angreifer es von Anfang an auf einen Automobilkonzern abgesehen, den die Mittelstand GmbH beliefert. Nachdem sich die Hacker mittels einiger perfekter Phishingmails Zugang zu den Computern der Buchhaltungsabteilung dieses Autoherstellers verschafft hatten, arbeiteten sie sich wie schon zuvor langsam, aber bestimmt weiter durch die Abteilungen vor. Nur durch den Zugriff auf die Infrastruktur der Mittelstand GmbH und die bei der Attacke gewonnen Informationen war es den Angreifern möglich, diese Phishingmails zu versenden. Einzig einem glücklichen Zufall ist es zu verdanken, dass der Angriff überhaupt bemerkt wurde: Nach dem Befall eines Rechners in der Buchhaltung des Automobilkonzerns mit einem drittklassig programmierten Virus wurde dieser Rechner von den firmeneigenen Sicherheitsspezialisten genauer untersucht. Obwohl dieser Virus ungefährlich war und mit dem eigentlichen, großangelegten Angriff nichts zu tun hatte, führte seine Entdeckung doch dazu, dass genauere Untersuchungen angestellt wurden. Bei diesen Kontrollen stießen die Spezialisten erst auf einige Ungereimtheiten und schließlich auf die Spuren des Angriffs, der vor zwei Jahren bei der Mittelstand GmbH begonnen hatte.

Zusammen mit den bald verständigten Behörden wurde schließlich ermittelt, dass sich der Angriff wohl am besten als „Advanced Persistent Threat“ (deutsch: „fortgeschrittene, andauernde Bedrohung“) klassifizieren lässt. Die Angreifer scheuten keine Kosten und Mühen, steckten wohl viele Monate in die Entwicklung und das Testen der Angriffssoftware. Die

Festnetztelefone, die die Mittelstand GmbH neu angeschafft hatte, dienten als erstes Einfallstor. Diese Telefone waren bereits vor deren Lieferung nach Deutschland mit einer veränderten Firmware bespielt worden, was klarmacht, über welche Mittel die Hacker verfügen müssen.

Bei den weiteren Untersuchungen des Angriffs offenbart sich außerdem, dass die Angreifer wohl mehrere sogenannte „Zero-Day“-Lücken ausnutzten, um sich innerhalb der Firmennetzwerke fortzubewegen. Bei „Zero-Day“-Lücken handelt es sich um Schwachstellen in Programmen, die der Öffentlichkeit und vor allen Dingen dem Hersteller der Software zum Zeitpunkt der Ausnutzung noch nicht bekannt sind. Diese Sicherheitslücken werden oftmals unter Hackern und Geheimdiensten gehandelt. Dieser Fakt zusammen mit der Expertise und den anderen Ressourcen, die die Angreifer zur Verfügung hatten, spricht dafür, dass die Attacke auch durch eine fremde Regierung mitunterstützt wurde. Dies ist für einen „Advanced Persistent Threat“ nicht ungewöhnlich.

„Sicherheit ist ein mehrdimensionales Thema – die Schaffung eines adäquaten Risikoniveaus in einer Organisation erfordert einen Mix aus organisatorischen, technischen und didaktischen Maßnahmen.“
David Ruge, Mittelstand 4.0 Kompetenzzentrum Stuttgart

Entstandener Schaden

- Unterwanderung der IT-Infrastruktur und Ermöglichung einer Straftat durch die eigene Infrastruktur.

Was ist passiert?
Advanced Persistent Threat – fortgeschrittene dauerhafte Bedrohung

Der Advanced Persistent Threat (APT) bezeichnet eine fortgeschrittene Variante eines Cyberangriffs. Im Gegensatz zu breitgefächerten Angriffen auf eine große Gruppe von potenziellen Opfern handelt es sich bei APT um eine gut vorbereitete, anhaltende Bedrohung, der ein Unternehmen ausgesetzt ist.

Der Angreifer nimmt bei APT einen hohen Ressourcenaufwand in Kauf und bereitet seinen Angriff über einen längeren Zeitraum vor. In vielen Fällen baut die Angriffsstrategie auf Social-Engineering-Elementen (siehe S. 13) sowie technischen Aspekten auf. In der Regel bleibt der Angreifer über einen längeren Zeitraum in einem System und schöpft Informationen zu neuen Produkten, strategischen Entscheidungen sowie anderen Werten eines Unternehmens ab.

Bei APT werden in der Regel fünf verschiedene Phasen unterschieden:

1. Zugang: Der Angreifer verschafft sich über eine infizierte Mail, eine Schwachstelle im Netzwerk oder eine mit Schadstoff versehene Smartphone-App Zugang zum System.

2. Fuß fassen: der Angreifer etabliert seinen Status im System, indem beispielsweise Teile der Systemsoftware manipuliert werden. So hat der Angreifer die Möglichkeit seinen Bewegungsradius im System unentdeckt zu erweitern.

3. Vertiefung des Zugangs: In dieser Phase des Angriffs versucht der Angreifer in der Systemhierarchie aufzusteigen, also möglichst Administratorenrechte zu erhalten. Dies geschieht oft über Social-Engineering-Strategien, die auf den im Vorfeld abgeschöpften Daten aufbauen.

4. Freies Bewegen: Ab einer bestimmten Hierarchiestufe im System hat der Angreifer die Möglichkeit, auf verwandte Systeme oder Subsysteme zuzugreifen.

5. Beobachten, Lernen und Bleiben: In dieser finalen Phase des Angriffs ist der Angreifer in der Lage, zentrale Teile des Systems und dessen Prozesse zu steuern.

Wichtig ist zu beachten, dass der Angreifer in manchen Fällen das System wieder verlässt. In der Regel tut er dies jedoch nicht, ohne sich einen Zugang (backdoor) zu bewahren. Auf diesem Weg kann ein regelmäßiger Abfluss essentieller Informationen eines Unternehmens (Neuentwicklungen, geplante Patente etc.) gewährleistet werden. Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) haben in der ersten Phase des APT die Verwendung von Installer- und Update-Hijacking („to hijack“, deutsch: „kapern“) stark zugenommen. Beim Installer- und Update-Hijacking werden Installations- und Updatepakete vom Angreifer so gekapert und manipuliert, dass sie die Schadsoftware des Angreifers installieren.

Die Motivationen hinter einem APT sind unterschiedlicher Natur und hängen stets vom Geschäftsmodell des Angreifers ab. In vielen Fällen handelt es sich um wirtschaftliche Spionage im Auftrag von inländischer Konkurrenz, ausländischen Staaten, die ihren Unternehmen einen Wettbewerbsvorteil verschaffen wollen, sowie von Akteuren, die nicht eindeutig einer dieser Gruppierungen zugeordnet werden können. Aufgrund des hohen Ressourcenaufwands, den der Angreifer bereit ist zu tätigen, kann immer davon ausgegangen werden, dass die substantiellen Werte eines Unternehmens betroffen sind.

Durch die starke Vernetzung des Wirtschaftens steigen die Risiken für APT, da in der Regel nicht alle Glieder einer Wertschöpfungskette das gleiche Sicherheitsniveau generieren. Deshalb werden oftmals Zulieferer infiltriert, über die das eigentliche Angriffsziel ins Visier genommen wird – man spricht in solchen Fällen von Lieferketten-Angriffen. Ein bekanntes Beispiel hierfür ist der sogenannte Stuxnet-Wurm, der 2010 entdeckt wurde. Es handelt sich um eine Schadsoftware, die sich über Zwischenstationen schließlich ihren Weg in ein Steuerungsprogramm der Firma Siemens suchte. Es wird vermutet, dass Stuxnet geschrieben wurde, um das iranische Atomprogramm zu sabotieren. Dazu sollten

„Vor allem kleine und mittlere Unternehmen stehen im Fokus von Cyberattacken. Zum einen verfügt der innovative Mittelstand über spezifisches Know-how, welches für Angreifer durchaus attraktiv ist. Zum anderen sind sie in die Lieferketten von Großkonzernen eingebunden und werden oft als Angriffsvektoren genutzt. Dass sich KMU tendenziell weniger umfassend schützen als Großkonzerne, kommt erschwerend hinzu.“

Teresa Ritter, Bitkom, Bereichsleiterin Sicherheitspolitik

„Damit man auf IT-Sicherheitsvorfäll reagieren kann, muss man sie erst einmal erkennen. Die kontinuierliche Überwachung des Netzwerks ist deshalb sehr wichtig.
Ingmar Baumgart, Leiter Kompetenzzentrum IT-Sicherheit

die Zentrifugen, die dort zur Anreicherung von Uran verwendet wurden, durch den Wurm zerstört werden. Einige Sicherheitsexperten schätzen, dass die Entwicklung von Stuxnet die aufwendigste und teuerste in der Geschichte der Schadprogramme (Malware) war.

Auch im Kontext von APT sollte Kontakt mit den zuständigen Stellen (siehe Anlaufstellen für Cybercrime auf S. 39) aufgenommen werden. Es empfiehlt sich außerdem, Maßnahmen so einzuleiten, dass der Angreifer zunächst keinen Verdacht schöpft. So ist es in einem späteren Stadium der Behebung des Problems möglich, den Angreifer in einer isolierten Umgebung gewähren zu lassen, um somit mehr über das Profil des Angreifers sowie seine Ziele zu erfahren.

Hilfestellungen

- Gegen manche Angriffe ist eine umfassende Absicherung nicht möglich, dies gilt wohl insbesondere für KMU, da diese nur begrenzte Ressourcen für die IT-Sicherheit aufwenden können. Man kann es allen potenziellen Angreifern jedoch so schwer wie möglich machen, indem man der IT-Sicherheit einen hohen Stellenwert zuweist. Immer mehr große Unternehmen fordern von ihren Zulieferern ein Mindestmaß an IT-Sicherheit, da die Gefahr besteht, dass ein Angriff über die schlecht gesicherte Infrastruktur des Zulieferers erfolgt. Verschiedene IT-Sicherheitsstandards kann man sich zum Beispiel durch eine ISO 27001-Zertifinzierung nachweisen lassen.
- Sehr wichtig ist es, die eigenen Prinzipien und Vorgehensweisen in Punkto IT-Sicherheit immer wieder zu evaluieren und entsprechend nachzubessern. Dazu sollte man auch immer auf dem Laufenden sein, welche Angriffsarten und Gefahren es gerade gibt. Hilfe können hier zum Beispiel folgende Produkte bieten:

- Phishing-Radar der Verbraucherzentrale[23] mit aktuellen Warnungen.
- Aktuelle Warnungen vor Viren, Würmern und anderen Sicherheitslücken des Bürger-CERT (Computer Emergency Response Team) des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[24].
- DsiN-Blog[25]: der IT-Sicherheitsblog für den Mittelstand
- SiBa[26] (Abkürzung für: Sicherheitsbarometer): App von „Deutschland sicher im Netz“, die Verbraucher über relevante Bedrohungen der digitalen Sicherheit informiert.

„Für kleine und mittlere Unternehmen ist es wichtig, ihre Kronjuwelen zu identifizieren und zu schützen. Das sind die Daten und Prozesse, die für das Unternehmen überlebenswichtig sind.“

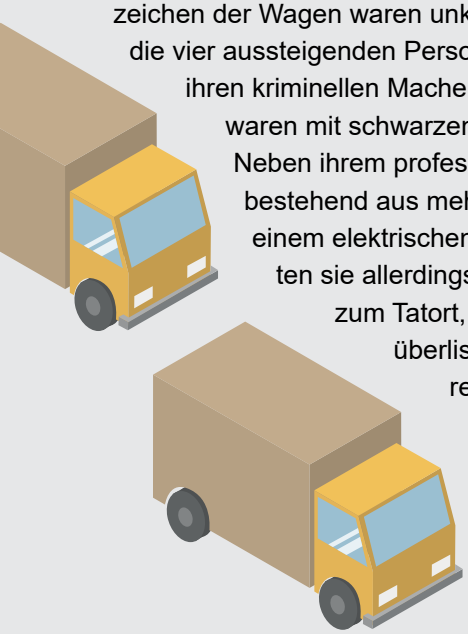
Sven Herpig, Projektleiter „Internationale Cyber-Sicherheitspolitik“ bei der Stiftung Neue Verantwortung

23 https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/phishingradar-aktuelle-warnungen-6059 (zuletzt aufgerufen am 20.05.20)
24 https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Buerger-CERT/Buerger-CERT_node.html (zuletzt aufgerufen am 20.05.20)
25 https://www.dsin-blog.de (zuletzt aufgerufen am 20.05.20)
26 https://www.sicher-im-netz.de/siba-unternehmen (zuletzt aufgerufen am 20.05.20)

Die Fertigungsabteilung

Eines Nachts werden bei der Mittelstand GmbH Fässer mit Chemikalien und andere Werkstoffe im Wert von mehreren Hunderttausend Euro entwendet. Die Ressourcen werden dringend für die Fertigung benötigt und so kommt es durch deren Fehlen zu einem mehrtägigen Ausfall der Produktion. Es entstehen erhebliche Kosten, die den Familienbetrieb in den finanziellen Ruin zu treiben drohen.

Mithilfe der Aufnahmen der Überwachungskameras wird schnell festgestellt, wie die Eindringlinge vorgingen. Wie in einem Gangsterfilm fuhren die Verbrecher gegen drei Uhr nachts mit zwei Kleinlastwagen vor dem Lager der Mittelstand GmbH vor. Die Kennzeichen der Wagen waren unkenntlich gemacht und die vier aussteigenden Personen, die sich sogleich ihren kriminellen Machenschaften widmeten, waren mit schwarzen Skimasken maskiert. Neben ihrem professionellen Equipment, bestehend aus mehreren Sackkarren und einem elektrischen Hubwagen, brachten sie allerdings auch Vorwissen mit zum Tatort, denn die Alarmanlage überlisteten sie durch die korrekte Eingabe des neunstelligen Sicherheitscodes – und das auch noch beim ersten Versuch.



Die Überwachungsvideos vermitteln zudem, dass sich die Diebe wohl sehr sicher gewesen sein müssen, dass sie ungestört bleiben würden, denn sie ließen sich für ihren Coup ganze eineinhalb Stunden Zeit. Sie müssen wohl gewusst haben, dass die Bilder der Überwachungskameras nachts nicht durch einen Menschen kontrolliert werden. Die Leitung der Mittelstand GmbH setzte wohl darauf, dass die Alarmanlage in Kombination mit der Abschreckungswirkung der Videokameras zur Sicherung des Gebäudes ausreichen würde.

Nach Beendigung ihrer diebischen Arbeit löschten die Eindringlinge außerdem das Licht, verschlossen das Rolltor und reaktivierten die Alarmanlage. All diese Tatsachen sprechen für eine organisierte Bande von professionellen Einbrechern. Verstärkt wird dieser Verdacht noch durch die Tatsache, dass sie wohl auch in Hinblick auf ihre Computerfähigkeiten nicht gerade auf den Kopf gefallen zu sein scheinen. Sich den Sicherheitscode für die Alarmanlage zu verschaffen, gehört wohl nicht gerade zum Repertoire des typischen Kleinkriminellen.

Einer der höher gestellten Mitarbeiter der Mittelstand GmbH erhielt am Vorabend des Einbruchs eine E-Mail, die vorgab, von der Sicherheitsabteilung des Betriebs zu stammen. Darin wurde er aufgefordert, seinen Sicherheitscode für die Werks-Alarm-

anlage routinemäßig zu ändern. Nach dem Klicken auf den Link in der Mail, der ihn auf eine seriös anmutende Internetseite mitsamt Mittelstand-GmbH-Logo und HTTPS-Verschlüsselung führte, wurde er aufgefordert den alten und seinen gewünschten neuen Sicherheitscode in eine Maske einzugeben. Nach dem Absenden des Formulars durch einen Mausklick wurde ihm versichert, dass der Vorgang nun abgeschlossen und der neue Sicherheitscode übernommen worden sei. Bei der verlinkten Internetseite handelte es sich jedoch um eine gefälschte Seite, der Sicherheitscode wurde durch die Eingaben des Mitarbeiters nicht geändert, sondern lediglich an die Verbrecher übermittelt, die diesen noch in derselben Nacht bei ihrem Einbruch verwendeten.

„Für den IT-Sicherheitsbereich werden oft Vergleiche aus der Automobilindustrie herangezogen – so wird beispielsweise oft behauptet, dass man kein Auto bauen können muss, um in der Lage zu sein, damit zu fahren. Diese Aussage ist grundsätzlich richtig. Sicherer wurde das Autofahren jedoch erst mit dem staatlich vorgeschriebenen Sicherheitsgurt, den Airbag-Systemen und einer sich ständig fortentwickelnden Straßenverkehrsordnung.“

David Ruge, Mittelstand 4.0 Kompetenzzentrum Stuttgart

Entstandener Schaden

- Diebstahl von Material im Wert von mehreren hunderttausend Euro.
- Erheblicher Schaden durch den mehrtägigen Ausfall der Produktion.

Was ist passiert?
Phishing – „nach Passwörtern angeln“

Der Neologismus Phishing setzt sich aus den englischen Wörtern „password“ und „fishing“ zusammen. Beim Phishing versuchen Angreifer über gefälschte E-Mails und Internetseiten an persönliche Informationen wie z. B. Passwörter zu gelangen. Das gefälschte Medium wird wie ein Netz ausgeworfen und versucht möglichst viele Passwörter und persönliche Daten aus dem Nutzerpool „herauszufischen“.

In der Regel gibt sich der Angreifer als vertrauenswürdiger Dienstleister (z. B. Netzbetreiber, Finanzdienstleister, staatliche Stelle o. ä.) aus und fordert dazu auf, persönliche Daten in eine dafür vorgesehene Maske einzugeben. In vielen Fällen werden vermeintliche Gründe wie die Aktualisierung der allgemeinen Geschäftsbedingungen oder die Umstellung im Sinne der Datenschutz-Grundverordnung angegeben, um dem Nutzer ein seriöses Anliegen vorzuspielen.

Die Täuschungsmails werden stets an das Corporate Design des Dienstleisters angepasst, sodass der Geschädigte nur schwer erkennen kann, ob es sich tatsächlich um eine vertrauenswürdige Nachricht handelt oder nicht. Zur Identifizierung von Phishingversuchen empfiehlt das Bundesamt für Sicherheit in der Informationstechnik (BSI) bei E-Mails insbesondere auf folgende Merkmale zu achten:

1. Absenderadresse: In der Regel nutzt der Absender leicht veränderte Absenderadressen, die der Nutzer nicht sofort erkennt (z. B. „info@paypol.de“ statt „info@paypal.de“).

2. Anrede: Dienstleister, die bereits in einem engen Kontaktverhältnis mit einer Person stehen, schreiben diese in der Regel mit Vor- und Nachnamen an. In Phishingmails findet meistens keine oder eine allgemeine Anrede statt.

3. Dringender Handlungsbedarf: Um beim Geschädigten eine Affekthandlung zu provozieren, wird signalisiert, dass die Eingabe der Daten sofort geschehen muss, da es sonst zu einem Verlust von Geld oder Daten kommt.

4. Drohungen: Ebenso wird dem Geschädigten oft gedroht, dass bei Nichteingabe der Daten die Sperrung des Kontos erfolgt.

5. Abfrage von vertraulichen Daten: Vertrauenswürdige Dienstleister fragen in der Regel keine Passwörter oder persönliche Identifikationsnummern in einer E-Mail ab.

6. Links und Formulare: In vielen Fällen werden in E-Mails Formulare verlinkt, die der Nutzer aufrufen muss, um seine persönlichen Daten einzugeben. Um sich effektiv schützen zu können, ist es in erster Linie erforderlich, zu lernen, wie man verdächtige Links identifiziert.

7. Sprache und Schrift: In manchen Fällen sind E-Mails in gebrochenem Deutsch verfasst. Dies hat den Hintergrund, dass die E-Mails maschinell übersetzt werden, um den Phishing-Radius zu erhöhen. Außerdem können sie ausländische Schriftzeichen enthalten bzw. sich durch das Fehlen von Umlauten auszeichnen.

Das Geschäftsmodell des Angreifers baut in der Regel darauf auf, dem Geschädigten einen direkten ökonomischen Schaden zuzufügen, beispielsweise durch die Abbuchung eines Geldbetrages. Bei mittelständischen Unternehmen kommt es im Zusammenhang mit Phishing-Attacken immer häufiger zur Auslösung kostspieliger Bestellungen im Bereich der Beschaffung.

Wenn sich der Angreifer in einem Land bewegt, das nur einen sehr eingeschränkten strafrechtlichen Zugriff ermöglicht, dann muss der Geschädigte davon ausgehen, dass er den ökonomischen Schaden selbst tragen muss. In jedem Fall ist der Kontakt zur Polizei geboten.

„Phishing Angriffe – egal ob breit gestreut oder gezielt – werden immer besser. Werden sie auf Grundlage echter, beispielsweise vorher bei einem Gesprächspartner entwendeter, E-Mails erstellt, haben die Opfer fast keine Chance mehr, sie noch rechtzeitig zu erkennen.“
Christoph Frohneberg, Disponent Cyberwehr Baden-Württemberg

Hilfestellungen

- Information der Verbraucherzentrale zum Thema: „Phishing und trojanische Pferde – Angriffe auf den eigenen PC erkennen und abwehren“[27].
- NoPhish[28]: Android Lernspiel zur Phishing Erkennung
- Phishing-Radar der Verbraucherzentrale[29] mit aktuellen Warnungen.
- TORPEDO[30]: Add-on, um Phishing-E-Mails zu erkennen
- „Wie Sie betrügerische Nachrichten und insbesondere Phishing-Nachrichten erkennen können“ (Flyer als pdf)[31].
- Das Bundesamt für Sicherheit in der Informationstechnik (BSI) über Spam, Phishing & Co (mit Video)[32].
- Das BSI speziell über Phishing (mit Video)[33].

„Der Faktor Mensch als Sicherheitsrisiko darf nie unterschätzt werden. Technische Sicherheitsmaßnahmen unterstützen, können aber ohne eine durch Sensibilisierung geschärfte Aufmerksamkeit wirkungslos werden.“

Sven Mattheis, Mittelstand 4.0 Kompetenzzentrum Saarbrücken

27 https://www.verbraucherzentrale.de/sites/default/files/2018-11/Phishing_und_trojanische_Pferde_Angriffe_auf_den_eigenen_PC_erkennen_und_abwehren.pdf (zuletzt aufgerufen am 20.05.20)
28 https://secuso.aifb.kit.edu/521.php (zuletzt aufgerufen am 20.05.20)
29 https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/phishingradar-aktuelle-warnungen-6059 (zuletzt aufgerufen am 20.05.20)
30 https://secuso.aifb.kit.edu/TORPEDO.php (zuletzt aufgerufen am 20.05.20)
31 https://www.aifb.kit.edu/images/1/19/KIT-Faltblatt-Online-Betrug.pdf (zuletzt aufgerufen am 20.05.20)
32 https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/spamPhishingCo_node.html (zuletzt aufgerufen am 20.05.20)
33 https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/phishing_node.html (zuletzt aufgerufen am 20.05.20)

Die AG IT-Sicherheit

Die Arbeitsgruppe IT-Sicherheit vernetzt die Mittelstand 4.0-Kompetenzzentren des Förderschwerpunkts „Mittelstand-Digital“. Geleitet wird die Arbeitsgruppe durch Dr. Frauke Goll und Dr. Thomas Usländer.

Das wichtigste Ziel der Arbeitsgruppe ist die Aufnahme von sicherheitsrelevanten Problem- und Fragestellungen aus den verschiedenen Wertschöpfungssegmenten sowie deren mittelstandsgerechte Aufarbeitung.

Zentrale Themen, die aktuell von der Arbeitsgruppe bearbeitet werden, sind „Sensibilisierung“ sowie „Risikoeinschätzung“. IT-Sicherheit ist jedoch ein „Moving Target“ – deshalb werden die Themen regelmäßig dem Bedarf der Kompetenzzentren und ihrem Anwenderkreis angepasst.

Neben der internen Vernetzung der Kompetenzzentren steht die Arbeitsgruppe in ständigem Austausch mit anderen Arbeitsgruppen des Forschungskonsortiums „Mittelstand-Digital“ sowie diversen Projekten der Initiative „IT-Sicherheit in der Wirtschaft“.

David Ruge
Koordinator der
AG IT-Sicherheit

Bei Fragen zur AG IT-Sicherheit
wenden Sie sich bitte an David Ruge.
E-Mail: ruge@fzi.de

Bildnachweis

Titel: Pixabay | S. 4–5 Icons designed von Rawpixel.com – Freepik.com | S. 6 Pixabay | S. 7 Pixabay, Tango Desktop Project | S. 8 Pixabay, Tango Desktop Project | S. 11 Pixabay | S. 15 Pixabay | S. 19 Pixabay, Tango Desktop Project | S. 27 © Rizky Djati Munggaran / 123RF.com | S. 33 Pixabay

Impressum

Herausgeber
Mittelstand 4.0-Kompetenzzentrum
Stuttgart c/o FZI Forschungszentrum Informatik
Haid-und-Neu-Straße 10-14
76131 Karlsruhe

Rechtsform
Das FZI Forschungszentrum Informatik ist eine Stiftung des bürgerlichen Rechts.

Stand
Okktober 2020

Druck
Fraunhofer Verlag
Mediendienstleistungen
Nobelstraße 12
70569 Stuttgart

Auflage
700

Was ist Mittelstand-Digital?

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Regionale Kompetenzzentren helfen vor Ort dem kleinen Einzelhändler genauso wie dem größeren Produktionsbetrieb mit Expertenwissen, Demonstrationszentren, Netzwerken zum Erfahrungsaustausch und praktischen Beispielen. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenlose Nutzung aller Angebote von Mittelstand-Digital. Weitere Informationen finden Sie unter www.mittelstand-digital.de.

Für den Notfall

Zentrale Ansprechstellen der Polizeien der Länder und des Bundes für die Wirtschaft

Die zentralen Anlaufstellen Cybercrime der Polizeien für Wirtschaftsunternehmen (ZAC)[34] nehmen Strafanzeigen von Unternehmen entgegen, sichern gegebenenfalls Beweise und bauen im Hintergrund einen konstanten Strafverfolgungsdruck auf die Täter auf.

Bundeskriminalamt
+49 611 55-15037
zac@cyber.bka.de

Baden-Württemberg
+49 711 5401-2444
cybercrime@polizei.bwl.de

Bayern
+49 89 1212-3300
zac@polizei.bayern.de

Berlin
+49 30 4664-924924
zac@polizei.berlin.de

Brandenburg
+49 3334 388-8686
zac@polizei.brandenburg.de

Bremen
+49 421 362-3853
cybercrime@polizei.bremen.de

Hamburg
+49 40 4286-75455
zac@polizei.hamburg.de

Hessen
+49 611 83-8377
zac.hlka@polizei.hessen.de

Mecklenburg Vorpommern
+49 3866 64-4545
cybercrime.lka@polmv.de

Niedersachsen
+49 511 26262-3804
zac@lka.polizei.niedersachsen.de
https://www.zac-niedersachsen.de/

Nordrhein-Westfalen
+49 211 939-4040
cybercrime.lka@polizei.nrw.de

Rheinland-Pfalz
+49 6131 65-2565
lka.cybercrime@polizei.rlp.de

Saarland
+49 681 962-2448
cybercrime@polizei.slpol.de

Sachsen
+49 351 855-3226
zac.lka@polizei.sachsen.de

Sachsen-Anhalt
+49 391 250-2244
zac.lka@polizei.sachsen-anhalt.de

Schleswig Holstein
+49 431 160-4545
cybercrime@polizei.landsh.de

Thüringen
+49 361 57431-4545
cybercrime.lka@polizei.thueringen.de

34 https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html (zuletzt aufgerufen am 20.05.20)

Zentrale Ansprechstellen ohne Legalitätsprinzip (Auswahl)

Das Legalitätsprinzip bezeichnet die Verpflichtung einer Strafverfolgungsbehörde, ein Ermittlungsverfahren einzuleiten, wenn der Verdacht besteht, dass eine Straftat erfolgt ist.

Im Umkehrschluss bedeutet das, dass eine Anlaufstelle, die nicht nach dem Legalitätsprinzip arbeitet, kein Ermittlungsverfahren einleiten muss. Inzwischen gibt es mehrere Anlaufstellen in Ergänzung zur Strafverfolgungsarbeit der Polizei. Sie unterstützen Unternehmen, damit sie nach einem IT-Sicherheitsvorfall möglichst zeitnah wieder einen geregelten Betrieb aufnehmen können. Es empfiehlt sich daher, sich bereits im Voraus in Ruhe zu informieren, wer im Fall der Fälle die benötigte Unterstützung leisten kann.

Die Liste der Ansprechstellen ohne Legalitätsprinzip wird bei Bedarf kontinuierlich erweitert und aktualisiert. Der aktuelle Stand findet sich unter www.mittelstand-gmbh.de.

Cyberwehr Baden-Württemberg
+49 800 292379347
https://cyberwehr-bw.de

Cyber-Allianz-Zentrum Bayern
+49 89 31201-222
caz@lfv.bayern.de

CERT-Hessen
CERT-Hessen/Bereich Cybersecurity
+49 611 353 9900
cert-hessen@hmdis.hessen.de
it-sicherheit@hmdis.hessen.de

AG Cybersicherheit
Senatsverwaltung für Inneres und Sport Berlin
+49 30 90223-2279
cybersicherheit@seninnds.berlin.de

Nordrhein-Westfalen
www.justizministerium-nrw.de/JM/schwerpunkte/zac

Sperr-Hotline für Kreditkarten, Girokarten und anderen Kartenzahlungsmitteln

Da man sich in der Regel die vielen Sperrrufnummern der verschiedenen Geld- und Kreditinstitute kaum merken kann, was gerade bei Zahlungsmitteln verschiedener Banken sehr kompliziert wird, gibt es mit der 116116 die erste weltweite zentrale Hotline, um Kreditkarten bei Verlust zu sperren. Die Sperrrufnummer ist 24 Stunden am Tag erreichbar und innerhalb Deutschlands gebührenfrei.

Sperr-Notruf:	116 116
aus dem Ausland:	+49 116 116