GDV Gesamtverband der Versicherer



Aus dem Schatten

Wie Hacker angreifen.
Wie sich Unternehmen schützen.

EIN CYBERKRIMI UND HANDBUCH ZUR IT-SICHERHEIT

„Sie machen kaum Arbeit, bringen aber ordentlich Geld ein. Das sind Shadows Lieblingsziele.“

Dieses Handbuch beschreibt, wie Unternehmen mit einfachen Schutzmaßnahmen und moderatem Aufwand deutliche Verbesserungen im Bereich der IT-Sicherheit erzielen können.

So gut wie alle aufgeführten Maßnahmen sind für mittelständische Unternehmen **schnell und effizient umsetzbar.**

Zusammen machen sie es Angreifern **deutlich schwerer**, das Unternehmensnetzwerk zu infiltrieren.

„Quick Wins", wie das Aktivieren von **Multi-Faktor-Authentifizierung** (siehe Infotext „Sichere Authentifizierung" auf Seite 37) oder der Einsatz von kostenfreier, qualitativer **Antivirensoftware** wie der „Windows-Sicherheit"-Suite (siehe Infotext „Schutz vor Schadsoftware" auf Seite 29) sind kostengünstig implementierbar und erzeugen nahezu keinen zusätzlichen Wartungsaufwand.

Darüber hinaus verdeutlicht das Handbuch, **welche Pflichten ein Unternehmen nach den unverbindlichen Musterbedingungen des GDV erfüllen sollte**, wenn es eine Cyberversicherung abgeschlossen hat (siehe Obliegenheiten des GDV auf Seite 46).

CYBER S!CHER

Eine Initiative der Versicherer

Mit der Initiative CyberSicher sensibilisieren die Versicherer für die Gefahren aus dem Cyberspace und zeigen, wie sich kleine und mittlere Unternehmen schützen können.

www.gdv.de/cybersicher

Ransomware ist die aktuell größte Bedrohung

Das Handbuch schildert im Folgenden einen **fiktiven Ransomware-Angriff**. Bei einem solchen Angriff verschlüsseln die Angreifer Unternehmensdaten und stellen das Schlüsselmaterial zur Wiederherstellung nur gegen eine Lösegeldzahlung bereit. Seite 5 zeigt die sechs Phasen eines typischen Ransomware-Angriffs, die wir im folgenden Szenario veranschaulichen.

Das Unternehmen Franz & Söhner GmbH gibt es genauso wenig wie die Hackergruppe Bad Guyz Inc. Doch das Szenario ist alltäglich und stellt aktuell das größte Cyber-Risiko für Unternehmen dar. Die hier geschilderten Angriffstechniken entstammen den zahllosen Ransomware-Vorfällen der vergangenen Jahre auf Unternehmen jeglicher Größe. Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sind „Angriffe mit Ransomware die größte Bedrohung für die Cybersicherheit in Deutschland“.[1] Das zeigte sich auch in Deutschlands erstem „digitalen Katastrophenfall“ im Juli 2021. Dabei wurde die Landkreisverwaltung von Anhalt-Bitterfeld (Sachsen-Anhalt) durch einen Ransomware-Angriff für 206 Tage lahmgelegt, sodass die Menschen im Landkreis weder Sozialleistungen beantragen noch ein Auto zulassen konnten.

Die Lösegeldforderungen der Cyberkriminellen bewegen sich je nach Unternehmensgröße bis in den mittleren neunstelligen Bereich, während die tatsächlichen Zahlungen im mittleren bis hohen sechsstelligen Bereich rangieren.[2] Neben den unmittelbaren Kosten für die Wiederherstellung des Geschäftsbetriebs können Ransomware-Angriffe auch die Reputation oder gar die Existenz des Unternehmens bedrohen. **Wie groß das tatsächliche Ausmaß der Schäden durch Ransomware ist, lässt sich aufgrund der hohen Dunkelziffer kaum sagen.**

Inhalt

Phase 1: **Reconnaissance** 7
Handlungsempfehlung:
Passwort-Leak-Management 12
Handlungsempfehlung:
Patch Management 12

Phase 2: **Initialer Zugriff** 14
Handlungsempfehlung:
Multi-Faktor-Authentifizierung und starke Passwörter 18

Phase 3: **Privilege Escalation** 20
Handlungsempfehlung:
Privileged Access Management 23

Phase 4: **Exfiltration** 24
Handlungsempfehlung:
Datenabfluss unterbinden 26

Phase 5: **Verschlüsselung** 27
Handlungsempfehlung:
Schutz vor Schadsoftware 29

Phase 6: **Mitigation** 31
Handlungsempfehlung:
Resiliente Datensicherungen und umfassende Wiederherstellungsplanung 34

Tipps & Technik 35
Obliegenheiten des GDV 46
Nachwort 48
Online-Verweise 49
Impressum 51



Phase 1
Reconnaissance

Wie Hacker ihre Ziele auswählen

„Nee, lass mal, ich will jetzt wirklich was tun“, sagt Shadow. Eben sind sie an der Ecke angekommen, an der es in seine Straße geht. Und jetzt bleibt auch Tr00per stehen.

„Sicher?“ Tr00per wollte eigentlich noch ein schnelles Bier mit seinem Kollegen trinken. Oder auch zwei oder drei.

„Ja, ernsthaft“, sagt Shadow, denn er hat heute richtig Lust zu arbeiten. „Der nächste Kunde sieht ganz nett aus. Könnte richtig gut werden.“

Tr00per weiß Bescheid – heute muss er sein Bier allein trinken. Auch er verdient sein Geld als Hacker. So haben die beiden sich kennengelernt, als Teil der Cybergang Bad Guyz Inc. Normalerweise haben die Mitglieder untereinander keinen persönlichen Kontakt, schon gar nicht in der echten Welt. Aber als beiden klar wurde, dass sie in derselben Stadt leben, haben sie sich doch angefreundet. Skaten, Bier trinken, feiern gehen. Dann wieder Unternehmen hacken, Daten verschlüsseln. Lösegeld erpressen. Das Geschäftsmodell von Bad Guyz Inc. ist recht einfach. Aber es lohnt sich.

„Ein neuer Kunde, wie schön!“, grinst Tr00per. „Staat? Energieversorgung? Dax?“ – „Solider deutscher Mittelstand“, antwortet Shadow. „Die sagen doch selbst immer, man müsse sich mehr um sie kümmern.“ Er dreht ab und ruft seinem Kumpel erst ein „Ciao!“ hinterher, als er ihn schon zwei Schritte hinter sich gelassen hat.

Denn Shadow hat einiges vor. Mindestens mit den Vorarbeiten, also Recherche und Datensammlung, will er fertig werden,

bevor die Sonne untergeht. Als Selbstständiger muss man sich die kleinen Deadlines selbst setzen, sonst kommt man zu nichts.

Von seinem neuen „Kunden“, der Franz & Söhner GmbH in Heilbronn, hat er vorher noch nie gehört. Er ist nur durch Zufall auf die Firma gestoßen. In einem seiner Lieblingsforen im DARKNET, wie es in den Nachrichtenmagazinen immer so geheimnisvoll genannt wird, hat Shadow sich eine Liste mit heimlich gestohlenen Zugangsdaten besorgt. Insgesamt mehrere Tausend Benutzernamen und die dazugehörigen Passwörter, darunter natürlich auch vielfach die Klassiker: „1234567“, „hallo“, „password“. Woher die LEAKS kommen, weiß er nicht. Will er auch gar nicht wissen. Er kennt den Verkäufer. Ehrenmann.

Darknet: verborgener Teil des Internets, in dem Nutzer vollkommen anonym agieren können

Shadow hat mit solchen Sammlungen in der Vergangenheit eigentlich immer irgendwo Glück gehabt. Die Login-Informationen führen auch dieses Mal fast überallhin: Windows-Anmeldedaten, Mail-Accounts, LinkedIn, X, Insta, Facebook, Amazon und ebay, aber auch Seitensprung-Portale und Pornoseiten. Mehr als genug Möglichkeiten, um Chaos zu stiften. Vor allem aber viele Chancen, mit einfachen Mitteln Geld zu machen. Viel Geld.

Leak (dt. Leck, Loch): nicht autorisierte Veröffentlichung von Informationen

Zum Beispiel mit Lutz Gernhardt und seinen Windows-Anmeldedaten: lutz.gernhardt@franzundsoehner.de und – ja, allen Ernstes – seinem Passwort „hall0123“. Gernhardt, das ergibt eine schnelle Google-Suche, die direkt zu seinem LinkedIn-Konto führt, ist seit rund einem Jahr als Systemadministrator bei Franz & Söhner beschäftigt. Und hat hoffentlich keine Ahnung, dass seine Daten auf Shadows Liste stehen.

Die Franz & Söhner GmbH, das ergibt Shadows Recherche, handelt von Baden-Württemberg aus mit gebrauchten Industriemaschinen, zum Beispiel Abfüll- oder Fertigungsanlagen. Die werden gebraucht gekauft, überholt und anschließend mit Gewinn wieder verkauft. Die Firma wurde vor 42 Jahren gegründet, ist ein Familienbetrieb in zweiter Generation, hat inzwischen 40 Angestellte. Ein Jahresumsatz von 5,2 Millionen Euro ist die

aktuellste Zahl, die Shadow finden kann. Für die Größe und das biedere Geschäftsmodell gar nicht übel.

Franz & Söhner betreibt eigentlich ein klassisches Offline-Business, was der etwas hemdsärmelige Geschäftsführer zum 40-jährigen Jubiläum in der Lokalzeitung nicht ohne Stolz betont hat. Aber auch die Franz & Söhner GmbH funktioniert natürlich nicht mehr komplett analog, sondern ganz im Gegenteil ziemlich digital.

Auch die Anbahnung und Abwicklung von Geschäften findet bei Franz & Söhner im Netz statt. Wobei die Firma nicht allzu viel in ihr IT-Know-how investiert hat. Stattdessen hat sie sich über verschiedene Dienstleister eine Website samt Webshop einrichten lassen, in dem sie den aktuellen Bestand, Angebote und Rechnungen verwalten kann.

Shadows Vermutung: Das Problembewusstsein für Cyberkriminalität wird bei Franz & Söhner nicht allzu groß sein. Er kennt das schon: Die meisten Mittelständler halten sich selbst gern für zu klein und zu unbedeutend, um in sein Visier zu geraten. Das sind Shadows liebste Ziele. Sie machen kaum Arbeit, bringen aber trotzdem ordentlich Geld ein. Viel besser als Dax-Konzerne, die sich mit allen Mitteln wehren und an denen man sich im Zweifel die Zähne ausbeißt.

Shadow macht sich einen Tee, knipst die Tischlampe an und schaltet den Fernseher ein. Allzu sehr muss er sich jetzt nicht mehr konzentrieren. Zur Entspannung ein paar Börsen- und Finanznachrichten, denn selbst hier bekommt er ab und zu Inspirationen für die nächsten Angriffe. Auch neue Start-ups, die schnell erfolgreich werden und viel Risikokapital einsammeln, haben oft keine vernünftigen ADMINISTRATOREN. Junge, begeisterte Leute, die von echter Sicherheit keinen Dunst haben. Weil sie gar nicht wissen wollen, wie schlecht die Welt da draußen eigentlich ist.

Administratoren (Abk. Admins): verwalten, warten und betreuen Computersysteme und haben dafür umfassende Zugriffsrechte

Shadow lächelt kurz vor sich hin, ihm gefällt der Gedanke. Dass er in dieser freien Wildbahn das Raubtier ist, das die schwachen Tiere sucht. Manche holt er sich gleich,

andere lässt er noch ein bisschen in Ruhe weiden. Bis er kommt. Er hat sie im Auge.

„Black Hats“ nennt man Leute wie ihn in der Fachsprache, Schwarzhüte. Wie im Western, um die guten von den bösen Cowboys zu unterscheiden. Böse heißt in diesem Fall: Shadow lebt vom Hacken, und das sogar sehr gut. Er ist kein klassischer Gangster mit Straßenerfahrung, er hatte noch nie eine Waffe in der Hand, er möchte niemandem wehtun – außer finanziell natürlich. Er sieht sich nicht wirklich als Verbrecher, trotzdem hat er sich mit den Jahren die kriminelle Logik draufgeschafft. Zum Beispiel: besser ein Tor nicht gewaltsam aufbrechen, sondern den Schlüssel beschaffen. Dann von innen zuschließen und das Schloss auswechseln. So ist am Ende nie er derjenige, der an die Tür hämmert. Das müssen dann die machen, denen das Haus eigentlich gehört.

Shadow schaltet den Fernseher wieder aus. Jetzt will er sich doch noch mal seinem neuen Kunden widmen. Mit den einfachen Techniken anfangen, um vielleicht heute Abend schon zu erfahren, ob er die komplizierteren überhaupt braucht.

Erster Versuch. Ein Besuch der Franz & Söhner-Website führt Shadow zum Login-Portal. Er lächelt. Wenn er hier als Administrator zugreifen kann, hat er ein ideales Einfallstor gefunden, um Zugriff auf die ganze digitale Infrastruktur der Firma zu bekommen. Er gibt die Zugangsdaten von Lutz Gernhardt ein. Fehlermeldung. Noch mal, vielleicht hat er sich nur vertippt. Wieder nichts. Mist. Das Passwort stimmt nicht mehr. Gernhardt hat es inzwischen geändert, vielleicht sogar als Reaktion auf den Leak.

Der ganz einfache und schnelle Hack wird es also leider doch nicht. Schade. Aber Shadow hat jetzt Blut geleckt. So schnell gibt er nicht auf.

Ein bisschen Lese- und Fleißarbeit ergibt, dass die IT-Abteilung wohl wirklich kein besonderes Augenmerk auf IT-Sicherheit hat, da die Website einige Informationen über die darunterliegende Infrastruktur verrät. So bekommt Shadow schnell einen Überblick über die eingesetzte Software – und damit Hinweise

auf mögliche Schwachstellen. Shadow ist sicher, dass er hier schnell fündig wird.

Und tatsächlich: Der Webshop von Franz & Söhner ist in JAVA geschrieben, und bei diesem Stichwort klingelt es bei Shadow sofort. Jeder Hacker kennt die Sicherheitslücke, die vor einiger Zeit im Java-basierten Protokollierungsprogramm Log4j entdeckt wurde. Ein perfekter Seiteneingang, der direkt in den Maschinenraum führt. Also: zweiter Versuch. Die passenden Log4j-Angriffstools hat Shadow natürlich zur Hand. Sie sind, wie die meisten Tools in seinem „Werkzeugkasten", öffentlich verfügbar und allseits bekannt. Shadow sucht auch nicht selbst nach neuen und unbekannten Schwachstellen, das ist ihm viel zu aufwendig – es reicht völlig, ein Opfer zu finden, das seine Schwachstellen nicht kennt oder einfach ignoriert.

Java: weitverbreitete Programmiersprache

Shadow ist guter Dinge. Der Webshop von Franz & Söhner läuft mit einer vergleichsweise alten Java-Version. Könnte klappen. Also: austesten. Aber auch Log4j hilft Shadow nicht weiter. Einer der IT-Dienstleister von Franz & Söhner hat rechtzeitig den rettenden Patch installiert. So hat Shadow keine Angriffsfläche mehr über Java, der Seiteneingang ist dicht.

Hmm. Den Idiotentest hat Franz & Söhner bestanden. Wäre auch zu schön gewesen, zu einfach, denkt Shadow. Er ist nur ein bisschen frustriert, er hat das schon oft erlebt. Aber jetzt kann er nicht mehr aufhören, er ist angefixt.

Es ist Donnerstagabend. Am Freitag dürfte – so wie er die Arbeitsmoral von deutschen Büroangestellten einschätzt – auch in Heilbronn nur noch bis mittags ernsthaft gearbeitet werden. Dann ist Wochenende. Das will Shadow aber nicht mehr abwarten. Daher wird er jetzt doch kurz die Ärmel hochkrempeln, obwohl er heute eigentlich nicht mehr viel tun wollte. Es gibt ein paar Vorbereitungen zu treffen. Er denkt wieder an seinen Raubtierinstinkt. Shadow will jetzt Fleisch.

ZUM NÄCHSTEN KAPITEL AUF SEITE 14



Handlungsempfehlung:
Passwort-Leak-Management

Informieren Sie sich über neue Passwort-Leaks, um im Falle eines Bekanntwerdens von Passwörtern schnell reagieren und die entsprechenden Zugangsdaten erneuern zu können. Dies ist insbesondere relevant, wenn Beschäftigte regelmäßig Benutzerkonten bei externen Diensten anlegen.

Hilfreiche Tools für diese Aufgabe sind die Identity Leak Checker des Hasso-Plattner-Instituts [3] und der Universität Bonn [4] sowie Have I been Pwned [5]. Die Dienste gleichen eine angegebene E-Mail-Adresse mit einer internen Leak-Datenbank ab und bieten in der Regel auch die Möglichkeit, den Nutzer zu alarmieren, sobald zukünftig eine Übereinstimmung gefunden wird.
Weitere Informationen zu Passwort-Leaks unten auf Seite 35.

Handlungsempfehlung:
Patch Management

Stellen Sie sicher, dass Ihr Unternehmen über ein vollumfängliches Patch Management für alle selbstverwalteten Systeme und Anwendungen verfügt. Dies sollte dafür sorgen, dass Sicherheitsupdates schnellstmöglich installiert werden, um die Risiken von neuen Schwachstellen zu minimieren. Unter Windows kann dies beispielsweise über eine Gruppenrichtlinie für alle Rechner erzwungen werden, während MacOS ähnliche Konfigurationsmöglichkeiten über das Device Management bereitstellt. Auch Linux-Systeme lassen sich so konfigurieren, dass Updates automatisch eingespielt werden.
Weitere Informationen zum Patch Management auf Seite 36 sowie in Obliegenheit 4 des GDV auf Seite 47.



Phase 2
Initialer Zugriff

Der gewaltsame Zutritt ins Unternehmensnetz

Kein vernünftiger Mensch schreibt mitten in der Nacht Mails. Höchstens Stalker, Burn-out-Kandidaten oder Leute in Europa, die mit Amerikanern Sachen zu klären haben, die nicht warten können. Aber sicher keine IT-Administratoren oder Systemdienstleister von süddeutschen Industriemaschinenhändlern. Wenn er seine Nachrichten an die Belegschaft von Franz & Söhner mitten in der Nacht abschicken würde, könnte seine schöne PHISHING-Aktion viel zu verdächtig aussehen.

Phishing: betrügerische Methode, bei der das Opfer dazu verleitet wird, sensible Daten (wie Anmeldedaten) preiszugeben

Manchmal hat Shadow in seinen Mails, mit denen er Leute hinters Licht führen will, Phrasen wie „Pardon für die späte Störung“ oder „Notfall – wie uns eben beim späten Back-up aufgefallen ist …“ eingebaut. Aber er hat keine guten Erfahrungen damit gemacht. Jedes unnötige Wort kann schlafende Hunde wecken. Dann gibt es Gebell. Bei seinen Phishing-Attacken bleibt Shadow daher möglichst unauffällig und spricht immer die ganze Belegschaft an. Ein einziger reicht. Und einen gibt es immer, der alle Anhänge öffnet, jeden Link klickt, überall seine Daten eingibt. Und diesen einen gibt es bestimmt auch bei Franz & Söhner.

Shadow weiß, dass die Firma größeren Ehrgeiz eigentlich nicht wert ist. Es gibt Hunderte, Tausende ähnliche Firmen, die einfacher zu knacken wären. Aber jetzt ist es zu spät. Er steckt zu tief drin in der Herausforderung. Er weiß: Er würde nachher nicht schlafen können, wenn er das nicht jetzt noch erledigt. Und: Er muss unbedingt ausnutzen, dass viele Beschäftigte am

Freitagvormittag etwas übereifriger sind als sonst. Schließlich soll zum Mittag möglichst alles erledigt sein.

Shadows Plan: Er wird sich in seiner Mailnachricht als Digitaldienstleister des Unternehmens ausgeben. Die Passwörter seien abgelaufen und müssten erneuert werden – das schütze schließlich gegen Hacker. Man solle doch bitte auf den folgenden Link klicken und dort sein Passwort ändern. Es ist ein tolles, paradoxes Spiel. Die Leute sollen Shadow ihre Informationen liefern, weil sie sich genau vor Leuten wie ihm schützen wollen.

Die Seite, auf die der Link in der Mail verweisen wird, sieht den internen Seiten von Franz & Söhner so ähnlich, dass niemand den Unterschied bemerken dürfte. Allerdings ist sie in Wahrheit nur ein täuschend echter Nachbau. Ein von Shadow mit einfachen Mitteln nachgeformter und ins Netz gepflanzter Doppelgänger, über den er die volle Kontrolle hat. Wenn die Gutgläubigen hier ihre Daten eintippen und dabei natürlich auch ihr vermeintlich altes Passwort eingeben, hat Shadow endlich, was er will: gültige Zugangsdaten für die IT-Infrastruktur von Franz & Söhner.

Social Engineering nennt sich die Disziplin, die ein guter Hacker beherrschen muss: die Fähigkeit, unbekannte Menschen da draußen dazu zu bringen, ihm zu glauben, ihre Daten, Informationen oder ihr Geld freiwillig herzugeben – und anschließend noch stolz auf sich zu sein, weil sie sich so korrekt verhalten haben. Shadow kennt die dilettantischen Mails voller Schreib- und Logikfehler, in denen andere Online-Banden vorgeben, Banken, Supermärkte oder Gewinnspielveranstalter zu sein. Selbst diese Betrüger sollen ja erstaunlich viel Erfolg haben.

Aber das kann er besser. Viel besser. Den größten Erfolg hatte Shadow mit einer Phishing-Mail an einem Jahresende: Die Belegschaft müsse sich in einem Portal einloggen und dort einen Antrag stellen, sonst würde der Resturlaub verfallen. Das Ergebnis: Innerhalb nur weniger Minuten gaben Dutzende ihre Zugangsdaten ein. Man muss die Menschen nur an der richtigen Stelle packen. Shadow muss ein bisschen lachen, als er sich daran erinnert. Er

stellt den Timer für seine Rundmail auf morgens um Punkt acht Uhr. Soll ja alles aussehen wie eine automatisierte Mail.

Nach einer kurzen Nacht und einem ersten Tee schaltet Shadow am nächsten Morgen den Bildschirm wieder ein. Und bekommt sofort gute Laune. Sein Köder hat gezogen. Von den 23 Mitarbeitenden der Firma, die er angeschrieben hat, haben zwölf auf den Link geklickt – und acht sogar ihre Zugangsdaten eingegeben. Besser kann es kaum laufen.

Shadow gibt die ersten Daten ein. Dann wird sein morgendlicher Enthusiasmus aber schneller gedämpft, als ihm lieb ist. Wie kann das sein? Nichts passt hier zusammen. Denn auf der echten, ungefälschten Login-Seite der Firma ploppt nach dem Anmelden mit E-Mail-Adresse und Passwort ein Fensterchen auf. Kurz fühlt er sich, als würde Lutz Gernhardt, der IT-Administrator, der unbekannte Mann in Heilbronn, ihn auslachen. Als würde er rüberwinken: Hast du dir so gedacht, was?

Eine Multi-Faktor-Authentifizierung, hier in Form einer zusätzlichen PIN an die Diensthandys? Bei Franz & Söhner? Im Ernst? Langsam wird Shadow doch richtig sauer. Wie kann es sein, dass die IT von Franz & Söhner so vorsichtig war und diese Hürde eingezogen hat? Mit den erbeuteten Daten kann er jedenfalls nichts anfangen, solange er nicht an die Codes kommt. Zudem könnte es sein, dass in der Firma langsam Verdacht aufkommt, wenn jemand Shadows Login-Seite als Fälschung erkannt hat.

Shadows Messenger blinkt. Eine Nachricht von Tr00per, ein Bierglas, ein Baum-Emoji und ein Fragezeichen. Ob er Lust hat, sich später im Park auf ein Bier zu treffen? Shadow antwortet. Ein stilisiertes Zifferblatt und ein rotes X. Heute wirklich keine Zeit, sorry.

Shadow muss jetzt schnell sein – und holt die Brechstange raus. Letzter Versuch. Wenn auch das nicht klappt, lässt er es gut sein. Für einen derart kleinen Fisch wie Franz & Söhner hat er sowieso schon zu viel Zeit investiert. Jetzt also noch eine Phishing-Attacke. Immerhin 12 von 23 Beschäftigten hatten den Link der ersten Mail angeklickt, da wird einer vielleicht auch

darauf reinfallen. Shadow nimmt eine seiner Vorlagen, eine angebliche Initiativbewerbung. Man glaubt nicht, wie neugierig viele Menschen sind. In der angehängten ZIP-Datei sind aber nicht nur der angekündigte Lebenslauf, das Anschreiben und die Zeugnisse, sondern auch Schadsoftware. Wird die Datei von einem Opfer geöffnet, wird sie sich automatisch mit der Infrastruktur von Bad Guyz Inc. verbinden und Shadow Zugriff auf die Systeme von Franz & Söhner geben.

Dann heißt es warten. Bis zum frühen Nachmittag passiert nichts, Shadow erwartet schon keine Reaktion mehr. Doch als er kurz nach 16 Uhr noch einmal kurz ins Projekt hineinschaut, kann er fast nicht glauben, was er da sieht.

ZUM NÄCHSTEN KAPITEL AUF SEITE 20

Handlungsempfehlung:
Multi-Faktor-Authentifizierung und starke Passwörter

Stellen Sie sicher, dass Ihr Unternehmen 1) Richtlinien für komplexe Passwörter mit einer Mindestlänge mithilfe technischer Maßnahmen einfordert und 2) durchgängig Multi-Faktor-Authentifizierung (MFA) verwendet. Dies gilt insbesondere für Dienste und Systeme, die direkt aus dem offenen Internet erreichbar sind.

Komplexe Passwörter verringern die Chance, dass Angreifer Passwörter systematisch erraten. MFA erschwert Angreifern den Zugang zum Unternehmensnetzwerk sogar dann, wenn diese bereits im Besitz von anderweitig erbeuteten, validen Zugangsdaten sind.

Weitere Informationen zur sicheren Authentifizierung auf Seite 37 sowie in den Obliegenheiten 1 und 2 des GDV auf Seite 46.



Phase 3
Privilege Escalation

Die Angreifer ziehen den Knoten zu

Es war ein heißer Tag in Heilbronn, und dann hatte Lutz Gernhardt auch noch quer durch die ganze Stadt gemusst. Eigentlich nur ein Chemistry Meeting mit einer zukünftigen Social-Media-Agentur, aber aus irgendwelchen Gründen hatte Marschke strikt darauf bestanden, dass er dabei sein sollte.

Natürlich, wie sich schnell herausstellte: Sie brauchen eigentlich keine Social-Media-Agentur. Und das hätten sie auch gut ohne den IT-Administrator rausfinden können. Gernhardt atmet laut durch die Nase aus, als er daran denkt, was er in der sinnlos vergeudeten Zeit alles hätte wegarbeiten können.

Das Gefühl der Erleichterung, als er wieder in seinem Büro im Franz & Söhner-Hauptgebäude angekommen ist, erscheint ihm selbst komisch. Er hätte auch gleich vom Meeting aus nach Hause fahren können. Aber da sind ja noch die neuen Tennisschläger, die hier am Schrank lehnen und von den Kids daheim sehnsüchtig erwartet werden. Gut, also doch ein schneller Blick in die Mails, die sich während seiner Abwesenheit angesammelt haben. Das Übliche. Standardfragen, CCs, Rundmails der Geschäftsführung, und sein Passwort muss erneuert werden. Schon wieder? Und dann vibriert auch noch sein Smartphone. Marschke wieder. Den Geschäftsführer kann er nicht warten lassen.

Gernhardt ist abgelenkt und tendenziell schon wieder spät dran, als er während des Gesprächs weiterscrollt und die Mail von Stephan Kurth sieht. Initiativbewerbung. Aha. Aber als was? Mal gucken, ob es sich lohnt, die Bewerbung an die Personal-Kollegin

weiterzuleiten. Schließlich sucht auch Franz & Söhner händeringend Fachkräfte.

„Ich muss prüfen, ob wir das so machen können“, sagt Gernhardt zu Marschke, während er die ZIP-Datei herunterlädt und öffnet, aber unter den ganzen Dokumenten das Anschreiben nicht sofort findet. Aber egal, jetzt ist Feierabend, alle warten schon auf ihn. Das hat Zeit bis nächste Woche. Er fährt seinen Rechner runter, schnappt die Schläger und fährt nach Hause.

Shadow würde gern sofort mit irgendwem anstoßen, als ihm klar wird, welchen Coup er da gelandet hat. Dummes Glück. Ausgerechnet Lutz Gernhardt ist auf seine Phishing-Mail hereingefallen und hat den Anhang geöffnet. Shadow stellt sich vor, wie sich seine Schadsoftware danach in kürzester Zeit tief ins System gegraben hat. Den Rechner des Administrators direkt mit seinem verbunden hat, eine Art Hotline. Völlig unverhofft ist er also doch noch ans Ziel gekommen. Er hat das Opfer zwischen den Zähnen. Jetzt muss er nur noch kräftig zubeißen, wenn Gernhardt seinen Rechner am kommenden Montag wieder hochfährt.

Will er das allein machen? Shadow greift zum Keyboard, öffnet den Messenger. Verschickt ein Geldsack-Emoji und ein Fragezeichen. Tr00per antwortet sofort mit einem strahlenden Smiley.

Nach einem langen Wochenende in ihren Lieblingsclubs beginnt die nächste Woche ungewöhnlich für Shadow und Tr00per. Sie orientieren sich an süddeutschen Bürozeiten und sitzen schon frühmorgens vor ihren Rechnern. Beide an ihren Schreibtischen, mit Standleitung über den Messenger. Wie sie sich genau im Allerheiligsten von Franz & Söhner bewegen und orientieren wollen, müssen sie erst mal sehen. Die Erfahrung sagt, dass jedes Unternehmensnetz anders aufgebaut ist und es eine ziemliche Herausforderung sein kann, die wirklich wertvollen Daten zu finden. Ein bisschen so, als wolle man in einer unbekannten Stadt das beste Restaurant am Platz finden, ohne Stadtplan, Tourismusblogs oder das Wissen der Einheimischen benutzen zu dürfen. Hacker wie Shadow und Tr00per profitieren von ihrer Erfahrung. Sie laufen immer dem Geruch nach.

Und die zwei haben wieder Glück. Auf dem infizierten Computer des Administrators findet Shadow die Zugangsdaten für ein weiteres, internes Login-Portal. Gernhardt hat Benutzername und Passwort offenbar erst vor Kurzem in die Kommandozeile eingetippt, über die Befehlshistorie sind sie leicht zu finden. An sich müsste es auch hier wieder eine Multi-Faktor-Authentifizierung geben, wie bei den am Vortag erfolglos ausprobierten System-Logins. Aber zur Überraschung von Shadow und Tr00per haben die Administratoren hier darauf verzichtet.

Wahrscheinlich ist es nach Ansicht der ITler von Franz & Söhner Schutz genug, dass das besagte Portal nur über einen VPN-Zugang erreicht werden kann. Was an sich keine verkehrte Idee ist: Gegen fremde Zugriffe übers Netz ist es damit gut gewappnet. Nicht allerdings gegen kompromittierte Firmencomputer wie den, den die zwei Hacker hier gerade unter ihre Kontrolle gebracht haben. Über ihn bekommen sie problemlos Zugang zum VPN und die dahinterliegenden Dienste.

VPN (Virtual Private Network): sichere, verschlüsselte Verbindung zwischen Rechnern und Servern über das ungeschützte Internet

Kurze Zeit später loggen sie sich über das Firmen-VPN direkt ins interne Portal ein. Das Stadttor führt sie so auf direktem Weg zur Tür des Palastes – und sogar mitten in ihn hinein. Tr00per ist offenbar aufgeregt, ständig blinkt der Messenger, während Shadow eher cool bleibt und irgendwann nicht mehr antwortet. Bloß nicht leichtsinnig werden. Abwarten und Tee trinken. Keine Energydrinks, keinen Kaffee, schon gar keinen Alkohol. Die Mission an sich ist stimulierend genug.

Und während Lutz Gernhardt in Heilbronn schon im Montagmorgen-Meeting sitzt, dringen die zwei Hacker still und leise in die Schatzkammer vor. Alles wie geplant, aber schneller als gedacht. Das BACKEND enthält in der Tat alle relevanten Kundendaten des Unternehmens, Liefer- und Rechnungsadressen, vergangene Bestellungen und sogar Einzelheiten über die Zahlungsabwicklung. Jackpot!

Backend (dt. hinteres Ende): technisch-administrativer Bereich einer Anwendung, der für Nutzer nicht sichtbar ist

ZUM NÄCHSTEN KAPITEL AUF SEITE 24



Handlungsempfehlung:
Privileged Access Management

Stellen Sie sicher, dass Ihr Unternehmen konsequent Nutzer- und Befugnisebenen unterscheidet und die entsprechenden Berechtigungen an separate Konten mit eigenen Zugangsdaten bindet. Administrative Konten sind ausschließlich für entsprechende Benutzergruppen anzulegen, die diese Konten dann auch nur für die Erledigung administrativer Tätigkeiten nutzen. So verhindern Sie, dass Angreifer mit übernommenen Benutzerkonten von anderen Beschäftigten weitreichende Schäden im Unternehmen anrichten können. **Weitere Informationen** zum Privileged Access Management auf Seite 39 sowie in Obliegenheit 1 des GDV auf Seite 46.

Phase 4
Exfiltration

Wie die sensiblen Daten aufgespürt und gestohlen werden

Manchmal muss Shadow daran denken, wie alles anfing. Wie ihm schon in seiner Kindheit klar war, dass er später etwas mit Rechnern machen wollte. Wie es ihm bald nicht mehr reichte, die Systeme nur zu verstehen. Er wollte sie durchdringen, zerbrechen, umordnen. Er wollte eigene Regeln schreiben.

Mit 14 zog er seinen ersten Hack durch. In der Schule. Er hatte die Arbeit der IT-Administratoren genau studiert und wusste, dass sie REMOTE-ZUGRIFF auf jeden PC im Netzwerk hatten. Bei der Lektüre war Shadow, der damals noch Lars hieß und keinen Kampfnamen hatte, auf das Thema Keylogger gestoßen: Software, die alle Tasteneingaben an einem Computer aufzeichnen und wiedergeben kann. Er installierte einen dieser Keylogger auf dem Bibliotheksrechner der Schule, kopierte die Dateien mit einer Remote-Administrationskonsole.

Remote-Zugriff (dt. Fernzugriff): Möglichkeit, von jedem Ort auf ein Gerät oder ein Netzwerk zuzugreifen

Theoretisch hätte er mit dem Wissen Zugriff auf seine Noten gehabt. Hätte sie löschen und sich selbst ein Topzeugnis ausstellen können. Hätte. Denn dazu kam es nicht. Er wurde erwischt und erhielt einen Verweis.

Später wollte Shadow eigentlich ein Held sein. Einer wie Julian Assange. Mit Daten Missstände und Skandale aufdecken, die Öffentlichkeit aufrütteln. Warnen. Dinge verändern. Während der Unizeit war das für seine Freunde und ihn noch eine valide Haltung, wenn sie sich auf größere Challenges vorbereiteten. Aber irgendwann änderte sich der Ansatz, von Grund auf. Als das Geld

mehr und mehr die Neugier abzulösen begann, wurde ihm das, was eigentlich in den Daten stand, mit der Zeit egal.

Heute gräbt Shadow immer noch gut abgeschirmte Informationen aus. Aber nur, um sie dann zu stehlen, zu verschlüsseln und ihre eigentlichen Besitzer zu erpressen. In einer Welt, in der komplette Existenzen und Lebenswerke auf Festplatten lagern, ist das eine ganz hervorragende Geschäftsidee.

Und genau das ist auch der Plan im Fall Franz & Söhner. Es ist nicht mal zehn Uhr, als Shadow im geknackten Verzeichnis die verfügbaren Datensätze überfliegt und dann damit beginnt, die Ordner mit den Kundendaten in seine eigene Infrastruktur zu übertragen. Während die Megabytes fließen, schaut er sich ein bisschen auf dem kompromittierten Server um – und entdeckt dabei einen weiteren Goldschatz, mit dem er nicht gerechnet hätte. Denn da ist eine Backup-APPLIKATION, die offenbar einmal am Tag eine Sicherungskopie der Daten anlegt und auf ein speziell dafür angelegtes Netzlaufwerk schiebt.

Applikation: Computersoftware, die eine bestimmte Funktion ausführt

Shadow kann sein Glück kaum fassen: Mit den Administratorenrechten von Lutz Gernhardt hat er jetzt auch vollen Schreibzugriff auf das Laufwerk, auf dem diese Backups liegen. Also auf genau die Kopien, die das Unternehmen für den Notfall anlegt, um ein gehacktes System wiederherstellen zu können. Tja, das wird diesmal wohl nichts, denkt sich Shadow, als er sich im Schreibtischstuhl kurz streckt.

Am liebsten würde er die wertvollen Daten-Backups des Unternehmens jetzt gleich löschen. Einfach so, sofort, weil er es kann. Es juckt ihn in den Fingern, denn ein bisschen Sadismus, ein bisschen Spaß an der Zerstörung verspürt er doch immer wieder mal. Doch er ermahnt sich, professionell zu bleiben. Noch muss er sich zurückhalten. Es wäre zu früh, die andere Seite auf sich aufmerksam zu machen.

Shadow schaut noch einmal nach. Nicht mehr lange, dann ist der Download der Daten abgeschlossen – und er kann bedenkenlos den Löschbefehl geben.

ZUM NÄCHSTEN KAPITEL AUF SEITE 27



Handlungsempfehlung:
Datenabfluss unterbinden

Stellen Sie mittels technischer Maßnahmen sicher, dass Schadsoftware nicht ungehindert mit dem Internet kommunizieren kann. Mögliche Strategien sind Firewalls auf Netzwerk- oder Anwendungsebene, die Schadsoftware daran hindern, Netzwerkverbindungen aufzubauen.

Die konfigurierten Regeln sollten regelmäßig daraufhin überprüft werden, ob sie noch den gewünschten Schutz bieten.

Weitere Informationen zu Application Firewalls auf Seite 42 sowie in den Obliegenheiten 2 und 3 des GDV auf Seite 46 und auf Seite 47.

Phase 5
Verschlüsselung

Der letzte Schritt: Daten werden unbenutzbar

Schamgefühl hat Shadow schon längst nicht mehr. Mitleid mit seinen „Kunden“ auch nicht. Schadenfreude trifft es eher. Natürlich gehört es zum Spiel, dass die Hacker den Corporate-IT-Leuten immer drei Schritte voraus sind, das wissen beide Seiten. Aber manche betteln wirklich darum, angegriffen zu werden. Die Leichtfertigkeit und Ignoranz, die ihm tagtäglich bei seinen geheimen Spaziergängen durch die Systeme anderer Leute begegnet, ist für Shadow manchmal kaum auszuhalten. Nein, Mitleid wäre nicht angebracht. Die Tränen soll man sich für die aufheben, die sie verdienen.

Mit Tr00per hat er sich am Vortag darüber unterhalten, wie hoch man im Fall von Franz & Söhner das Lösegeld ansetzen soll, also die Summe, die man von der Firma verlangen könne, um im Gegenzug die verschlüsselten Daten wieder freizugeben. 150.000 Euro, meinte Tr00per. „Ist ja am Ende eine kleine Klitsche.“ – „Nee“, antwortete Shadow. „Die brauchen doch gerade einen guten Rat von uns. Und der ist teuer. Der ist schon 250.000 wert, würde ich sagen. Außerdem hatte ich mit denen mehr Aufwand als sonst, deshalb der Zuschlag für schwierige Kunden.“

Nachdem er die Daten vollständig in seine Servercloud übertragen hat, beginnt Shadow, sein Werk zu vollenden. Zuerst gibt er den Befehl an die Schadsoftware, die Daten auf den Rechnern von Franz & Söhner zu verschlüsseln. Er schaut ein bisschen dabei zu, es ist immer wieder schön zu sehen: wie sich die Endungen der Files nach und nach wie von Zauberhand in kryptische Symbole verwandeln.

Die Lösegeldforderung hat er in eine Textdatei gepackt, die er mehrfach in die Datenordner legt. Shadow will die 250.000 Euro in Bitcoin, zahlbar an sein anonymisiertes Wallet. Was Bitcoin ist, sollte ja bis zum analogen Maschinenhandel durchgedrungen sein. Wie man sie bekommt, schreibt er sicherheitshalber auch gleich ins Erpresserschreiben.

Bleiben nur noch die Backups auf dem Netzlaufwerk. Das macht Shadow persönlich und in Handarbeit. Die konkret eingesetzten Applikationen und die Backup-Architektur haben von Unternehmen zu Unternehmen zu viele Eigenheiten, um das Löschen der Files automatisch laufen zu lassen. Aber diese Arbeit macht er gern. Als alle Sicherungskopien gelöscht sind, überschreibt er das Netzlaufwerk mit irgendwelchen anderen Daten, die er gerade zur Hand hat, einige Male sogar. Aus diesem Datenmüll wird Franz & Söhner garantiert keine Daten mehr wiederherstellen können, beim besten Willen nicht.

Shadow schaut auf die Uhr und durchs Fenster in die Sonne. Das passt ja alles prima. Sein Skateboard lehnt an der Tür. Heute wird er mit Tr00per gern im Park ein paar Bier trinken.

ZUM NÄCHSTEN KAPITEL AUF SEITE 31

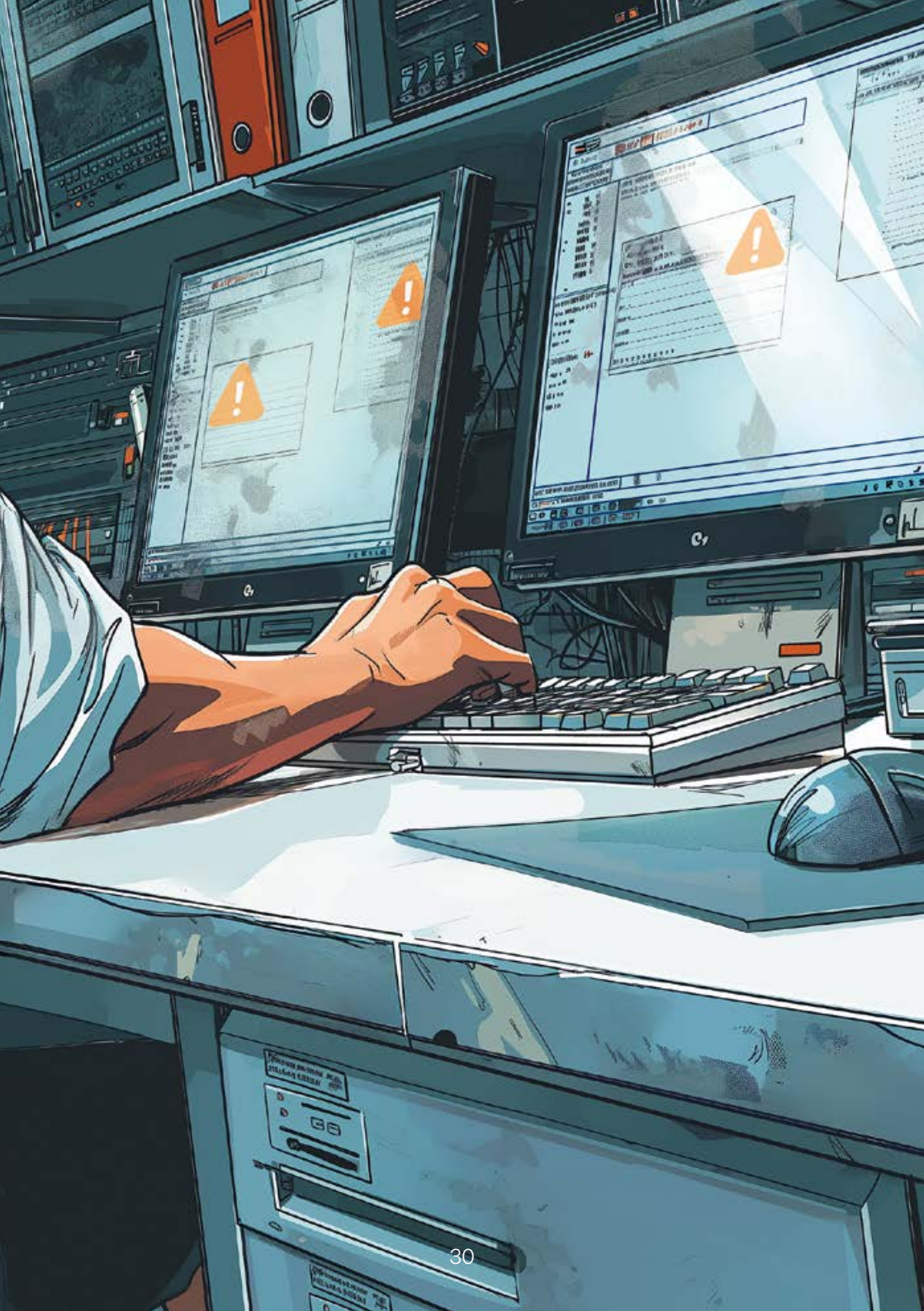
Handlungsempfehlung:
Schutz vor Schadsoftware

Stellen Sie mittels technischer Maßnahmen sicher, dass Schadsoftware wie Viren, Würmer und Trojaner nicht ungehindert auf Endgeräten oder Servern ausgeführt werden kann. Mögliche Strategien sind hierbei der Einsatz von Antivirensoftware (AV), weiter reichende Endpoint-Detection-and-Response(EDR)-Lösungen oder die konsequente Umsetzung von Code-Signierung im gesamten Unternehmen.

Die eingesetzten Sicherheitsapplikationen (ebenso wie das Betriebssystem und weitere Software) müssen stets aktuell gehalten werden, um potenzielle Schäden durch neue Bedrohungen zu minimieren.

Microsoft liefert mit dem Windows-Betriebssystem die Software-Suite „Windows-Sicherheit“ [6] (unter anderem bestehend aus Defender Antivirus und Defender Firewall) aus, die einen Basisschutz bereitstellt. Von diesem Schutz sollten Sie Gebrauch machen und sicherstellen, dass die Signaturen aktuell gehalten werden.

Weitere Informationen zum Schutz vor Schadsoftware auf Seite 42 sowie in den Obliegenheiten 2 und 3 des GDV auf Seite 46 und auf Seite 47.



Phase 6
Mitigation

Wie Unternehmen auf Ransomware-Angriffe reagieren

Nein, er kann die Kinder heute doch nicht von der Schule abholen. Auch nicht einkaufen. Es wird spät. „Esst heute Abend ohne mich“, sagt Lutz Gernhardt seiner Frau Marlene. „Tut mir leid!“

„Was ist denn los?“, fragt Marlene. Sie ist verärgert, aber auch besorgt. „Ist die Firma in die Luft geflogen?“ – „Tut sie vielleicht noch“, antwortet Lutz Gernhardt.

Er hat Montage nie gemocht. Aber dieser ist noch mal anders. Fast minütlich kommen neue TICKETS bei der IT an. Immer mehr Beschäftigte und Kunden von Franz & Söhner haben Probleme. Mit dem Webshop, mit den Mails, mit dem Rechnungswesen, mit den internen Verwaltungsportalen. Auch Geschäftsführer Marschke hat Probleme mit seinem Login. Der öffnet natürlich kein Ticket, sondern bellt direkt aus Gernhardts Telefon heraus. „Kümmern Sie sich darum. Und zwar sofort!“

Ticket: Ein IT-Ticketsystem verwaltet Anforderungen und Aufträge an die IT-Abteilung

Schon beim ersten Blick ins System wird Gernhardt klar, was los ist. Die kryptischen Datei-Endungen können nur eines bedeuten: Franz & Söhner wird attackiert, mit einem Ransomware-Angriff. Dann findet Gernhardt auch die Lösegeld-Forderung. Er atmet tief aus und ruft den Geschäftsführer an.

Was passiert ist, muss er Marschke kurz darauf im hektisch vereinbarten Krisentreffen erklären, mit so wenig Panik wie möglich. Dass es Eindringlinge im System von Franz & Söhner gibt. Profis, nicht etwa Script-Kiddies oder andere Amateure. Dass die Vandalen einiges kaputtgemacht hätten, das Problem aber im Laufe des Tages lösbar sei.

Gernhardt ist zuversichtlich. Er hat schließlich vorgesorgt. Das System legt jeden Tag Backups der wichtigsten Daten auf einem getrennten Netzlaufwerk an – um genau für solche Fälle gerüstet zu sein. Das kann der Firma heute 250.000 Lösegeld sparen – eine lohnende Investition also, findet Gernhardt.

Als er auf dem Laufwerk aber keine Daten, sondern nur Datenmüll findet, wird ihm heiß und kalt. Wie soll er das Marschke erklären? Am besten erst mal gar nicht. Bevor er sich eine Sprachregelung überlegt, um dem Chef auch diese Wahrheit schonend beizubringen, versucht er es bei seinen IT-Dienstleistern. Aber nach zwei Stunden Zoom-Calls auf seinem privaten Smartphone gibt es keinen Zweifel mehr: Die wichtigsten Daten von Franz & Söhner sind nicht nur weg, sondern weg weg. Futsch. Verschwunden. Zerstört. Vernichtet. Verloren. Wenn am Dienstag alles wieder gut sein soll, muss es ein anderer Dienstag sein.

Die Hauptfrage, die sich nach der gemeinsamen Tiefenanalyse stellt: Was wird es kosten, die Datenbanken und das digitale System der Firma auf eigene Faust wiederherzustellen? Welcher Umsatzverlust entsteht in dieser Zeit, in der Franz & Söhner praktisch handlungsunfähig ist? Bei Franz & Söhner weiß man das alles nicht, mit einem IT-Notfallplan hat sich in der Firma nie jemand beschäftigt. Das rächt sich jetzt. Alle Aufwände können nur grob geschätzt werden. Heraus kommt eine Summe, die das Lösegeld fast günstig erscheinen lässt. Also doch das Lösegeld einfach bezahlen und weitermachen, als wäre nichts passiert?

Marschke positioniert sich schnell und klar. Egal, was es kostet, man werde vor den Erpressern nicht einknicken. Erstens könne man nie sicher sein, dass nach der ersten Forderung nicht gleich eine zweite und dritte komme und das Geld schlicht in den Wind geschossen sei. Zweitens ermutige man damit ja nur die Kriminellen, immer so weiterzumachen. Nicht mit Marschke. Er beauftragt Gernhardt mit der Wiederherstellung der Systeme und stellt Strafanzeige gegen unbekannt.

Am Dienstag gibt es zumindest eine halbwegs gute Nachricht. Ein inzwischen beauftragter Dienstleister kann rudimentäre

Backup-Kopien wiederherstellen, die auf einem anderen Server liegen. Die enthalten aber nicht alle verlorenen Daten. Offene Rechnungen, Personal-Infos und einige andere Posten sind unvollständig. Außerdem dauert es einige Zeit, die zerstörte interne Infrastruktur nachzubauen. Rund zwei Wochen lang dürfte es bei Franz & Söhner wohl eher keinen Regelbetrieb geben.

Lutz Gernhardt weiß inzwischen, dass er derjenige war, der die Schadsoftware heruntergeladen hat. Er kann es nicht fassen. Marschke lacht nur bitter, als er hört, dass ausgerechnet sein IT-Administrator auf die Hacker reingefallen ist. Die Dienstleister stellen derweil – neben hohen Rechnungen – auch ein Lastenheft für eine bessere IT-Sicherheit in der Zukunft auf: Mitarbeiter schulen, Admin-Rechte sparsam nutzen, Backups vom Netzwerk trennen, mehr als eine Datensicherung anlegen, die Wiederherstellung der Datensicherung auch mal testen. Eigentlich das kleine Einmaleins der IT-Sicherheit – das aber die wenigsten Firmen sicher beherrschen. Franz & Söhner hat auf die ganz harte Art gelernt, was das im Ernstfall bedeutet.

Dass die Franz & Söhner GmbH am Ende schon nach zehn Tagen wieder am Netz ist, dass sie nur knapp am Kollaps vorbeischrammt und massive Auftragsverluste, Vertragsstrafen und immense Mahngebühren für zu spät bezahlte Rechnungen erleidet – all das bekommt Shadow gar nicht mehr mit. Als ihm klar wurde, dass Franz & Söhner das Lösegeld nicht zahlt, ist die Leidenschaft für den Fall bei ihm schnell abgeklungen. Er hat in der Zwischenzeit längst andere „Kunden“ gefunden – denn davon gibt es immer genug.

Handlungsempfehlung:
Resiliente Datensicherungen und umfassende Wiederherstellungsplanung

Stellen Sie sicher, dass kritische Unternehmensdaten einem engmaschigen Sicherungsprozess unterzogen werden, der mindestens wöchentlich durchgeführt wird. Die geschriebenen Datensicherungen sollten dabei im Idealfall 1) nicht von den gesicherten Systemen aus verändert oder gelöscht werden können, 2) physisch getrennt von den gesicherten Systemen sein und 3) unter strenger Zugriffskontrolle stehen.

Um etwaige Probleme im Wiederherstellungsprozess nicht erst im Ernstfall zu erkennen, sollten Sie diesen Prozess regelmäßig testen und verbessern. Ein Notfallwiederherstellungsplan, der die involvierten Systeme und Prozesse detailliert beschreibt, sollte integraler Bestandteil des Sicherheitskonzepts Ihres Unternehmens sein.

Weitere Informationen zu Datensicherungen auf Seite 43 sowie in Obliegenheit 5 des GDV auf Seite 47.

Tipps & Technik

Passwort-Leaks

Zugangsdaten und insbesondere deren Passwörter sind ein wertvolles Ziel für Angreifer, da sie in der Regel Zugriff auf Unternehmensressourcen ermöglichen. Im Darknet haben sich daher regelrechte Marktplätze etabliert, in denen Cyberkriminelle unter anderem Passwörter aus früheren Sicherheitsvorfällen zum Kauf anbieten. Diese sogenannten Leaks sind vor allem dann kritisch, wenn dieselben Passwörter für mehrere Dienste genutzt werden: Dann kann ein Angreifer mit einem Satz Zugangsdaten beispielsweise Zugriff auf einen Webshop und ebenso auf das E-Mail-Konto des Opfers bekommen.

Auch wenn Ihre Beschäftigten in der Regel keine externen Dienste mit der Unternehmens-E-Mail-Adresse nutzen, sollten Sie regelmäßig überprüfen, ob Zugangsdaten mit Ihrer E-Mail-Domain in solchen Leaks gefunden wurden. So können Sie der Passwort-Wiederverwendung vorbeugen und potenziell betroffene Zugangsdaten schnell ändern. Nutzen Sie dafür zum Beispiel den Dienst haveibeenpwned.com, der bekannte Leaks indiziert und abfragbar macht. Für Unternehmen besonders interessant ist die Funktion der Domain-Überwachung. Damit können Sie alle E-Mail-Adressen Ihres Unternehmens gebündelt überwachen und werden alarmiert, wenn diese in einem Leak auftauchen. Eine Alternative stellt die Uni Bonn mit dem „Leak Checker"-Dienst unter https://leakchecker.uni-bonn.de [4] zur Verfügung.

Idealerweise hat Ihr Unternehmen einen strukturierten und größtenteils automatisierten Prozess im Falle eines Alarms, mit dem betroffene Mitarbeitende informiert und zum Wechseln ihrer Zugangsdaten aufgefordert werden. Dies verhindert, dass potenzielle Angreifer die erbeuteten Zugangsdaten für weitere Dienste (intern und extern) nutzen können.

Umfassendes Patch Management

Ein strukturiertes Patch Management, das ein zeitnahes Einspielen von verfügbaren Sicherheitsupdates garantiert, ist ein essenzieller Baustein in der Cybersicherheitsstrategie jedes Unternehmens. Sobald ein Sicherheitsupdate für ein Betriebssystem oder eine Applikation verfügbar ist, können Angreifer es untersuchen, die behobene Schwachstelle rekonstruieren und oft auch ausnutzen.

Je nach Kritikalität und Art der Schwachstelle können so im schlimmsten Fall komplette Systeme aus der Ferne übernommen werden. Bei der bekannten Log4j-Schwachstelle, die im Dezember 2021 veröffentlicht und behoben wurde, dauerte es beispielsweise nur neun Minuten, bis erste Angreifer die Lücke ausnutzten und erste Systeme übernahmen.[7]

Stellen Sie daher sicher, dass Sicherheitsupdates im Idealfall sofort oder (in größeren Umgebungen) mit minimaler Testphase zeitnah im gesamten Unternehmen ausgerollt werden. So minimieren Sie die vermeidbaren Schäden einer ungepatchten Schwachstelle. Eine absolute Sicherheit garantiert aber auch das zeitnahe Einspielen von Updates nicht. Denn Lücken, für die noch keine Updates existieren, können weiterhin ausgenutzt werden. Deswegen sollte das Patch Management durch weitere Maßnahmen ergänzt werden, etwa durch Firewalls.

Sollte es in Ihrem Unternehmen kritische Applikationen geben, die keine Sicherheitsupdates mehr erhalten, aber für den allgemeinen Geschäftsablauf unerlässlich sind, sollten Sie diese nur unter strengen Schutzmaßnahmen und (falls möglich) abgeschottet in einem eigenen Netzwerksegment betreiben.

Schwachstellen-Newsfeeds

IT-Security-Newsfeeds informieren regelmäßig über aktuelle Bedrohungen, neue Sicherheitslücken und Updates. Mit ihrer Hilfe hat das IT-Sicherheitspersonal einen schnellen Überblick über die aktuelle Lage und kann proaktiv Angriffe verhindern.

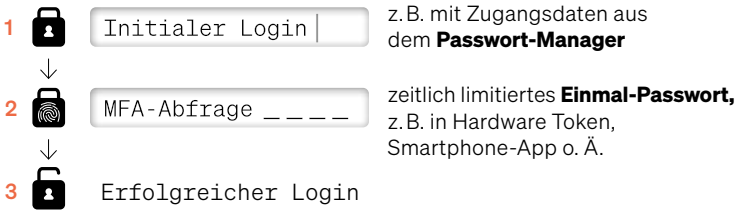
Beispiele für solche Newsfeeds sind die Angebote der Computer Emergency Response Teams (CERTs) oder Newsletter der Hersteller eingesetzter Produkte. Auf dem deutschsprachigen Markt existieren auch Nachrichtenanbieter wie Heise oder Golem, die regelmäßig über sicherheitsrelevante Themen berichten.

Sichere Authentifizierung

Sichere Authentifizierung ist elementar für die Sicherheitsstrategie eines jeden Unternehmens. Abbildung 1 (s. u.) bietet einen Überblick über einen Authentifizierungsprozess, der sichere Passwörter sowie eine konsequente Multi-Faktor-Authentifizierung umfasst. Ein sicheres Passwort zeichnet sich durch eine hohe Komplexität beziehungsweise Entropie aus, um das Passwort vor einem systematischen Erraten, dem sogenannten Brute Forcing, zu schützen. Die Entropie wird dabei entgegen verbreiteter Meinung primär von der Länge des Passworts – und nicht der Anzahl an Zahlen oder Sonderzeichen – bestimmt. So ist beispielsweise das Passwort „correct horse battery staple“ mit einer Entropie von circa 44 Bit komplexer und damit sicherer gegen Brute-Force-Angriffe als das umständlichere Passwort „Tr0ub4dor&3“, welches lediglich eine Entropie von circa 28 Bit aufweist.

Für die Umsetzung von sicheren Passwörtern in Ihrem Unternehmen sollten Sie daher technische Maßnahmen ergreifen, die eine gewisse Mindestlänge von Passwörtern erzwingen. Das häufige Ändern von Passwörtern wird hingegen nicht mehr empfohlen. Der regelmäßige Wechsel wird Ihre Mitarbeitenden dazu verleiten, möglichst kurze Passwörter zu verwenden und bei Variationen auf einfache Abwandlungen wie aufsteigende Zahlen am Ende eines Passworts zurückzugreifen.

Abbildung 1 · **Prozessschritte der Multi-Faktor-Authentifizierung**



Um Mitarbeitenden die Benutzung dieser langen Passwörter einfacher zu machen, empfiehlt sich der Einsatz von Passwort-Managern. Diese Programme sind in der Lage, eine unbegrenzte Menge an Passwörtern sicher zu speichern und diese Passwortsammlung mit einem einzigen Master-Passwort zu verschlüsseln. Die Mitarbeitenden müssen sich nun also lediglich ein

einziges, zur Sicherheit möglichst langes und nur für den Passwort-Manager genutztes Passwort merken und haben damit Zugriff auf alle im Unternehmen benötigten Passwörter.

Während eine hohe Passwortkomplexität die Passwörter vor Brute-Force-Angriffen schützt, können diese jedoch natürlich auch anderweitig in die Hände von Angreifern gelangen (siehe auch Infobox „Passwort-Leaks“ auf Seite 35). Die Multi-Faktor-Authentifizierung (MFA) schützt auch in diesem Szenario. Dem Authentifizierungsprozess wird ein zweiter Schritt hinzugefügt, in dem Ihre Beschäftigten neben den gültigen Zugangsdaten aus Nutzername und Passwort einen weiteren Faktor präsentieren müssen, um sich erfolgreich zu authentifizieren. Ein etabliertes Verfahren dafür sind Time-Based One-Time Passwords (TOTPs), die in Software (beispielsweise in einer App für Android oder iOS) oder auch in Hardware Token, wie speziellen USB-Sticks, generiert werden können



Exkurs:

Authentifizierung per Kryptografie

Als Alternative zu Passwörtern wird aktuell versucht, die Authentifikation von Benutzern über Kryptografie durchzuführen. So zielen Apples „Passkey“-Initiative oder das „FIDO2-Framework“ darauf ab, die Sicherheit und Benutzerfreundlichkeit von Authentifizierungsmethoden zu verbessern. Bei Apples Passkey ersetzt ein asymmetrischer kryptografischer Schlüssel das traditionelle Passwort, wodurch das Risiko von Phishing-Angriffen und Passwortdiebstahl reduziert wird. Der private Schlüssel bleibt sicher auf dem Gerät des Benutzers gespeichert. Ebenso verfolgt das FIDO2-Framework einen Ansatz, der eine starke Authentifizierung ohne Passwörter ermöglicht, indem es auf biometrische Daten oder physische Sicherheitsgeräte setzt. Diese Technologien signalisieren einen Paradigmenwechsel in der Art und Weise, wie wir uns authentifizieren, und zeigen auf, dass zukünftige Sicherheitslösungen vermehrt auf innovative kryptografische Methoden setzen werden, um die digitale Identität der Benutzer besser zu schützen.

Privileged Access Management (PAM)

Privileged Access Management (PAM) beschreibt einen umfangreichen Prozess zur Trennung, Kontrolle und Überwachung von administrativen Tätigkeiten, die innerhalb eines Unternehmens durchgeführt werden. PAM umfasst dabei Technologien und Applikationen sowie definierte Prozesse, die manuelle sowie automatisierte administrative Tätigkeiten verwalten und auditierbar machen.

Die Grundlage bildet das Prinzip der niedrigsten Berechtigungen (engl. „principle of least privilege"). Es besagt, dass Nutzer lediglich die Berechtigungen erhalten, die unbedingt notwendig sind, um ihre regulären Aufgaben zu erfüllen. So sollten beispielsweise Nutzer, die primär via E-Mail kommunizieren und Office-Tätigkeiten erfüllen, nur Standard-Benutzerrechte besitzen und selbst auf ihren eigenen Geräten keine lokalen administrativen Berechtigungen besitzen. Wird ein solches Gerät kompromittiert (etwa mittels eines Malware-Anhangs einer Phishing-E-Mail), ist der direkte Schaden erst einmal begrenzt auf das lokale System und die Daten, auf die der Nutzer Zugriff hat.

Weiterhin sollten Administratoren zwei Benutzerkonten haben: ein reguläres Benutzerkonto ohne besondere Rechte und ein weiteres Administratorkonto (mit eigenen Zugangsdaten und MFA), das nur für administrative Aufgaben verwendet wird. Zur Unterscheidung kann ein Suffix eingesetzt werden: max.muster@company.de und max.muster.admin@company.de. Diese Trennung der Accounts und deren Privilegien ermöglicht, dass die erweiterten Berechtigungen nur dann eingesetzt werden, wenn sie für eine entsprechende Aufgabe benötigt werden.

Neben dieser Trennung setzt Ihr Unternehmen im Rahmen des PAM idealerweise auch eine Audit-Schnittstelle um, die es möglich macht, administrative Tätigkeiten nachzuverfolgen und zu überwachen. So kann im Ernstfall transparent nachvollzogen werden, welche Aktivitäten Angreifer mithilfe von kompromittierten Konten durchgeführt haben. Im Zusammenspiel erschwert ein konsequent umgesetztes PAM, im Unternehmensnetzwerk Schäden anzurichten, die über einzelne kompromittierte Systeme oder Benutzerkonten hinausgehen.



Exkurs:

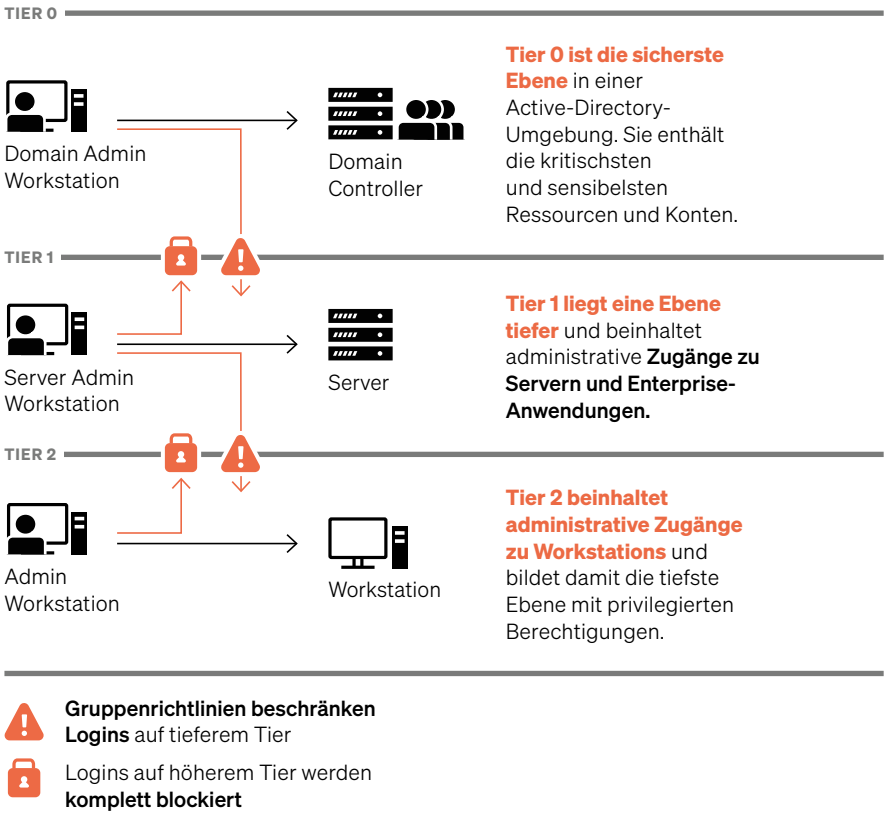
Härtung von Microsoft Active Directory (AD)

Die Härtung einer Lightweight-Directory-Access-Protocol(LDAP)- und Active-Directory(AD)-Konfiguration ist entscheidend für die Sicherheit und

Stabilität eines Unternehmensnetzwerks. Hierbei spielen verschiedene Maßnahmen eine zentrale Rolle, darunter LDAP Signing, LAPS (Local Administrator Password Solution) und AD Tiering.

LDAP Signing ist ein essenzieller Sicherheitsmechanismus, der gewährleistet, dass die Kommunikation zwischen einem LDAP Client und einem AD Domain Controller verschlüsselt und signiert ist. Dadurch wird die Integrität der Datenübertragung sichergestellt und vor möglichen Man-in-the-Middle-Angriffen geschützt. In der Standardkonfiguration ist diese Einstellung deaktiviert. Ohne LDAP Signing können Angreifer in der Regel mit einfachen Mitteln Kontrolle über die gesamte AD-Umgebung erlangen. Mehr Details finden sich im Microsoft Advisory ADV190023. [8]

Abbildung 2 · **Die drei Sicherheitsschichten der Active Directory**



Die Local Administrator Password Solution (LAPS) ist eine weitere wichtige Maßnahme zur Absicherung von Active Directory. Mit ihr werden die lokalen Administrator-Passwörter auf den Endgeräten im Netzwerk zufällig generiert und regelmäßig aktualisiert. Dies verhindert, dass ein kompromittiertes Administrator-Passwort auf mehreren Geräten eingesetzt werden kann, was die Angriffsfläche erheblich reduziert und die Sicherheit des Netzwerks erhöht.

AD Tiering ist ein Ansatz zur Segmentierung von Active Directory in verschiedene Sicherheitszonen oder Ebenen (Tiers). Durch die strikte Trennung von kritischen und weniger sensiblen Ressourcen können Zugriffsrechte gezielter gesteuert und potenzielle Angriffspfade minimiert werden. Dadurch wird das Risiko von unautorisierten Zugriffen auf sensible Daten deutlich reduziert. Abbildung 2 (Seite 40) gibt einen Überblick über eine typische AD-Tiering-Konfiguration mit den entsprechend segmentierten Ebenen und Zugriffsbeschränkungen. Effektives AD Tiering besteht aus drei Ebenen mit Login-Beschränkungen zwischen den Ebenen.

Application Firewall

Die Erkennung und Prävention von Exfiltrationsversuchen ist nicht trivial, da Angreifer sich in der Regel standardisierter Protokolle wie HTTPS oder SFTP bedienen. Diese werden mit hoher Wahrscheinlichkeit auch für die normale Kommunikation von Diensten im Unternehmen verwendet. Da Angreifer jedoch gerade bei Ransomware-Angriffen vor der Verschlüsselung der Daten auf eine schnelle Exfiltration abzielen, kann eine Erkennung basierend auf der Übertragungsgeschwindigkeit erfolgreich sein. Hierbei können Anomalien in der übertragenen Datenmenge Anzeichen für eine laufende Exfiltration sein.

Eine weiter reichende Möglichkeit, eine Exfiltration zu erkennen und zu verhindern, ist eine Application Firewall, die richtlinienbasiert entscheidet, welche Netzwerkverbindungen ein Prozess aufbauen kann. Im Gegensatz zu klassischen Firewalls für eingehende Verbindungen arbeitet eine Application Firewall prozesszentrisch und überwacht die ausgehenden Verbindungen, die ein Prozess anstößt. Die Standardrichtlinie ist dabei, Verbindungen von unbekannten Prozessen entweder komplett zu verbieten (Whitelisting-Ansatz) oder den rechtmäßigen Benutzer des Systems vor dem Verbindungsaufbau zu fragen. Hier sollten Beschäftigte geschult sein, unbekannte Verbindungen zu blockieren und zu melden. In beiden Fällen (Whitelisting und Benutzerabfrage) wird verhindert, dass Schadsoftware ungehindert Daten abrufen oder auch weiteren Schadcode nachladen kann.

Schutz vor Schadsoftware

Antivirensoftware (AV) und Endpoint Detection and Response (EDR) sind entscheidende Instrumente im Bereich der Cybersicherheit, die Unternehmen vor verschiedenen Bedrohungen schützen.

Antivirensoftware identifiziert und blockiert schädliche Software beim Versuch, in das Unternehmensnetzwerk einzudringen. Durch kontinuierliche Echtzeitschutzmaßnahmen überwacht AV den Datenverkehr, überprüft Dateien auf schädlichen Code, erkennt verdächtige Aktivitäten und blockiert diese sofort. Automatisierte Updates halten die Software aktuell und gewährleisten, dass sie gegen die neuesten Bedrohungen gewappnet ist.

Im Gegensatz dazu konzentriert sich Endpoint Detection and Response (EDR) auf die Überwachung von Endgeräten wie Computern und Laptops. EDR erkennt ungewöhnliche oder verdächtige Aktivitäten auf diesen Geräten, die

auf mögliche Angriffe hinweisen können. EDR ermöglicht nicht nur das Erkennen, sondern auch eine schnelle Reaktion auf Sicherheitsvorfälle, indem es etwa infizierte Geräte isoliert und Angriffe eindämmt.

Darüber hinaus bieten EDR-Produkte Funktionen für forensische Analysen, indem detaillierte Informationen über Sicherheitsvorfälle gespeichert werden. Auf Basis dieser Daten können die Ursachen und Auswirkungen von Angriffen gründlich untersucht und Maßnahmen zur Prävention zukünftiger Angriffe umgesetzt werden. EDR-Tools nutzen auch fortschrittliche Verhaltensanalysen, um Anomalien zu erkennen, die auf eine Bedrohung hindeuten könnten. Diese Funktionen ermöglichen eine umfassende Sicherheitsstrategie, die nicht nur auf traditionellen Computern, sondern auch auf mobilen Geräten angewendet werden kann.

Weiterhin existiert mit Code Signing ein Sicherheitsmechanismus in Microsoft Windows und Apple MacOS, um die Integrität und Authentizität von Software zu gewährleisten. Dabei wird der Programmcode digital signiert, um sicherzustellen, dass er nicht verändert wurde und tatsächlich vom Hersteller stammt. Als Nutzer ist es wichtig, auf die Signaturhinweise zu achten, die bei der Installation von Software angezeigt werden. In Windows wird dies oft durch eine Benachrichtigung angezeigt, die bestätigt, dass die Software von einem verifizierten Entwickler stammt. Auf MacOS zeigt das Betriebssystem eine ähnliche Meldung an, um die Echtheit der Software zu bestätigen.

Es ist ratsam, Software nur von vertrauenswürdigen Quellen herunterzuladen und zu installieren, um die Gefahr von Malware oder bösartiger Software zu minimieren. Wenn eine Software keine gültige Signatur aufweist oder von einem unbekannten Entwickler stammt, sollte man vorsichtig sein und im Zweifelsfall die Installation abbrechen.

Die Kombination von Antivirensoftware, Endpoint Detection and Response sowie Code Signing schafft ein robustes Sicherheitsnetzwerk, das Unternehmen vor einer Vielzahl von Cyberbedrohungen schützt. Durch frühzeitige Erkennung, schnelle Reaktion und kontinuierliche Überwachung können potenzielle Schäden minimiert und die Integrität von Unternehmensdaten und -systemen aufrechterhalten werden.

Datensicherungen

Datensicherungen (engl. „backups“) und deren Management sind zentrale Punkte einer Cybersicherheits- und Notfallstrategie. Ein gut durchdachtes und ständig zu optimierendes Backup Management sollte zum Ziel haben,

den Kern des Geschäftsbetriebs auch im Krisenfall kontinuierlich aufrechtzuerhalten, um den wirtschaftlichen Schaden zu minimieren. Die dafür notwendigen Daten, Prozesse und Systeme müssen im Vorhinein identifiziert und dokumentiert sein, um sie im Wiederherstellungsprozess priorisieren zu können. Das Backup Management sollte als Teil einer umfassenden Sicherheitsstrategie betrachtet werden, die vor Datenverlust durch verschiedene Szenarien schützt und die Integrität und Verfügbarkeit von Unternehmensdaten gewährleistet. Dabei gibt es einige zentrale Fragen, die maßgeblich beeinflussen, wie effektiv die Backups im Ernstfall genutzt werden können.

Was wird gesichert? Nicht alle im Unternehmen anfallenden Daten und nicht jedes beliebige System können wiederhergestellt werden. Viele Daten und teilweise ganze Systeme sind unkritisch für den minimalen Geschäftsbetrieb. Ein typischer Büroangestellter arbeitet an seinem Rechner beispielsweise in der Regel mit Dokumenten, die auf zentralen Fileshares oder Cloudspeichern abgelegt werden, und mit E-Mails, die ebenfalls redundant auf dem E-Mail-Server des Unternehmens (oder des Dienstleisters) gespeichert sind. Ein solches System kann unter Umständen von einer Sicherung ausgenommen sein, da alle wichtigen Daten anderweitig gespeichert und damit Teil des dortigen Backups sind. Das senkt den Bedarf an Ressourcen, die für den Sicherungsprozess erforderlich sind, und beschleunigt die Wiederherstellung, da kritische Systeme priorisiert werden können.

Wann wird gesichert? Das richtige Sicherungsintervall leitet sich aus der Kritikalität der Daten und den zu erwartenden Änderungen ab. Grundsätzlich gilt: Kritische Daten wie Kundendaten oder Daten essenzieller Geschäftsprozesse sollten in kürzeren Intervallen gesichert werden, während für selten geschriebene Daten tendenziell längere Intervalle toleriert werden können. Das Intervall sollte dabei individuell für einzelne Systeme/Systemgruppen definiert werden, um den verschiedenen Anforderungen gerecht zu werden.

Dabei ist zwischen inkrementellen Backups (die lediglich die Änderungen zu einem vorher erstellten Backup abbilden) und vollen Backups (die eigenständig wiederherstellbar sind) zu unterscheiden. Es ist empfehlenswert, inkrementelle Backups für kürzere Intervalle (beispielsweise täglich) zu wählen, während volle Backups in größeren Abständen geschrieben werden (beispielsweise wöchentlich). Das hat zwei Vorteile: Zum einen sind die häufigen Backups schnell abgeschlossen. Zum anderen ist sichergestellt, dass maximal zwei Wochen an Daten verloren gehen, sollte das letzte volle Backup fehlerhaft sein.

Wo und wie werden Backups abgelegt? Die Sicherungskopien sollten redundant und verschlüsselt auf externen Systemen und Datenträgern abgelegt werden, damit Angreifer die Backups nicht manipulieren können. Mindestens eine Kopie sollte sich nicht im selben Gebäude oder Rechenzentrum wie die anderen befinden, um vor Naturgewalten geschützt zu sein. Die räumliche Trennung (engl. „offsite backup") garantiert, dass in der Regel mindestens eine Kopie der Daten unbeschädigt für eine Wiederherstellung verfügbar ist. Aber Vorsicht: Beachten Sie, das Material zum Entschlüsseln der Daten unabhängig von den Backups zu lagern, um den Zugriff auf die Daten nicht zu verlieren!

Um die Backups vor Manipulation oder Zerstörung durch Angreifer zu schützen, verwenden Sie idealerweise sogenannte Append-only-Medien, die nur einmal geschrieben (jedoch vielfach gelesen) werden können. Dies stellt sicher, dass Angreifer einmal geschriebene Sicherungen nicht rückwirkend manipulieren können. Einen Schritt weiter gehen Offline-Medien, also Medien, die nach dem Schreiben vom Lesegerät getrennt und separat gelagert werden.

Wie wird die Wiederherstellung getestet? Die beste Wiederherstellungsstrategie kann im Notfall fehlschlagen, wenn sie nicht ausgiebig getestet und optimiert wurde. Um Probleme im Ablauf oder den Daten selbst nicht erst im Ernstfall zu erkennen, sollten Sie bei den Tests die Daten tatsächlich wiederherstellen und dies nicht nur simulieren. So reicht es in der Regel nicht, die betreffenden Backups zu entpacken und zu entschlüsseln, da in diesem Fall potenzielle Probleme bei der tatsächlichen Wiederherstellung der Systeme nicht erkannt werden können.

Abbildung 3 · **Die sieben wichtigsten Eigenschaften einer effektiven Sicherungsstrategie**

Eigenschaft	Umsetzung
Unveränderbar	Write/Append-only-Datenstrukturen; Schutz vor Manipulation (tamper-proof)
Unabhängig	Dedizierte Infrastruktur nur für Sicherungen
Isoliert	Eigenes Identity & Access Management (IAM) sowie strenge Zugriffskontrollen
Versioniert	Vorhaltung von mehreren Versionen je nach Wiederherstellungsanforderungen
Verifiziert	Regelmäßige Ende-zu-Ende-Wiederherstellungstests
Überwacht	Überwachung der erfolgreichen Erstellung von validen Sicherungen
Risiko-basiert	Priorisierung nach Kritikalität im Geschäftsprozess

Obliegenheiten des GDV

1. **Der GDV empfiehlt, ein umfassendes Identitätsmanagement zu implementieren, das konsequent Nutzer und dazugehörige Befugnisebenen unterscheidet.**

Jeder Nutzer sollte einen individuellen Zugang mit regulären Benutzerrechten erhalten. Administratoren erhalten zusätzlich dedizierte privilegierte Zugänge für jede Befugnisebene, die ihnen zugeordnet ist. Diese sind ausschließlich zur Erledigung von administrativen Tätigkeiten zu nutzen.

Weiterhin ist sicherzustellen, dass alle (!) verwendeten Passwörter eine ausreichend hohe Komplexität aufweisen. Dies kann in der Regel über eine Mindestlänge der verwendeten Zeichen erreicht werden.

Weitere Informationen: „Sichere Authentifizierung“ auf Seite 37 und „Privileged Access Management“ auf Seite 39.

2. **Der GDV empfiehlt, Mobilgeräte und Server, die aus dem Internet erreichbar sind, über zusätzliche Schutzmaßnahmen gegen unberechtigten Zugriff abzusichern.**

Diese Schutzmaßnahmen umfassen sowohl Ansätze gegen unberechtigten Fernzugriff als auch gegen physischen Zugriff. Konzepte wie Multi-Faktor-Authentifizierung (MFA), zertifikatsbasierte Anmeldung oder der Einsatz von Firewalls und Intrusion-Detection-Systemen erschweren den Fernzugriff und sind vor allem für Server geeignet. Mobilgeräte wie Smartphones, Tablets oder Laptops sollten eine Diskverschlüsselung aufweisen und idealerweise über grundlegenden Diebstahlschutz verfügen. Auch wenn „Find My Device“-Dienste von Apple oder Google nicht zu 100 Prozent verlässlich sind, können sie dabei helfen, einen Diebstahl zu detektieren.

Weitere Informationen: „Schutz vor Schadsoftware“ auf Seite 29 und „Sichere Authentifizierung“ auf Seite 37 und .

3. **Der GDV empfiehlt, umfassende Schutzmaßnahmen gegen Schadsoftware einzusetzen, die automatisiert gepatcht und so auf dem neuesten Stand gehalten werden.**

Dies umfasst neben klassischen Virenscannern und Anwendungs-Firewalls, die Schadsoftware auf Endgeräten erkennen und deren Kommunikation verhindern, auch alternative Ansätze wie den konsequenten Einsatz von Codesignierung, um bereits die Ausführung von unbekannter Software zu verhindern.

Weitere Informationen: „Schutz vor Schadsoftware“ auf Seite 29 und „Application Firewall“ auf Seite 42.

4. **Der GDV empfiehlt, ein Patch-Management-Verfahren zur konsequenten Verwaltung aller im Unternehmen eingesetzten Software zu implementieren.**

Das Ziel des Verfahrens ist die zeitnahe Installation aller verfügbaren Sicherheitsupdates sowohl für Betriebssysteme als auch für Anwendersoftware und Apps. Nur so können Sicherheitslücken durch bekannt werdende Schwachstellen schnell geschlossen werden. Falls Software eingesetzt werden muss, die keine Sicherheitsupdates mehr erhält, sollten betroffene Systeme so gut wie möglich isoliert und durch zusätzliche Schutzmaßnahmen gesichert werden, etwa durch Netzwerkisolation und Firewalls.

Weitere Informationen: „Umfassendes Patch Management“ auf Seite 36.

5. **Der GDV empfiehlt, wichtige Unternehmensdaten einem mindestens wöchentlichen Sicherungsprozess zu unterziehen.**

Die genaue Ausgestaltung des Sicherungsprozesses hängt stark von den zu sichernden Daten und den weiteren Gegebenheiten im Unternehmen ab. Jedoch sollten Sicherungen idealerweise 1) regelmäßig physisch getrennt von den zu sichernden Daten verwahrt werden, 2) nicht nachträglich veränderbar sein und 3) regelmäßig inklusive des Wiederherstellungsprozesses getestet werden.

Weitere Informationen: „Datensicherungen“ auf Seite 43.

Nachwort

Das fiktive Szenario rund um den Angriff auf die Franz & Söhner GmbH illustriert, an wie vielen Stellen Cyberkriminelle potenziell gestoppt werden können. Auch wenn ein vollständiger Schutz nicht möglich ist: Je mehr Sicherungsmaßnahmen umgesetzt werden, desto besser. Denn Angreifer, insbesondere Ransomware-Gruppen, versuchen ihre Zeit optimal zu nutzen. Sie lassen in der Regel von ihrem Ziel ab, wenn sie zu viele Schutzmaßnahmen vorfinden und sie zu viel Zeit investieren müssten, um ihre Schadsoftware ausrollen zu können. Das Ziel der IT-Sicherheitsstrategie sollte daher immer dasselbe sein: Das Schutzniveau so zu erhöhen, dass der Ernstfall gar nicht erst eintritt.

Online-Verweise

1 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html
2 https://www.coveware.com/ransomware-quarterly-reports
3 https://sec.hpi.de/ilc
4 https://leakchecker.uni-bonn.de/de/index
5 https://haveibeenpwned.com
6 https://support.microsoft.com/de-de/windows/gesch%C3%BCtzt-bleiben-mit-windows-sicherheit-2ae0363d-0ada-c064-8b56-6a39afb6a963
7 https://blog.cloudflare.com/exploitation-of-cve-2021-44228-before-public-disclosure-and-evolution-of-waf-evasion-patterns
8 https://msrc.microsoft.com/update-guide/en-us/advisory/ADV190023

GDV

Aus dem Schatten – Ein Cyberkrimi und Handbuch zur IT-Sicherheit
Herausgeber
Gesamtverband der Deutschen Versicherungswirtschaft e. V.
Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020–5000
Fax: +49 30 2020–6000
www.gdv.de, berlin@gdv.de

Verantwortlich
Oliver Hauner
Leiter Cyberversicherung
Dr. Maurits Helmich
Referent Cyberversicherung
cyberversicherung@gdv.de

Autor/-innen
Joachim Hentschel,
Dr. Tobias Müller,
Security Research Labs,
Dr. Florian Wilkens,
Security Research Labs

Layout und Produktion
twotype design, Christian Hruschka

Titelbild
Montage twotype design mit Motiven von Midjourney

Illustrationen
Midjourney

Disclaimer
Dieses Handburch stellt eine allgemeine, unverbindliche Information dar. Die Inhalte wurden mit der erforderlichen Sorgfalt erstellt. Gleichwohl besteht keine Gewährleistung auf Vollständigkeit, Richtigkeit, Aktualität oder Angemessenheit der darin enthaltenen Angaben oder Einschätzungen. Eine Verwendung liegt in der eigenen Verantwortung des Lesers.

GDV 2025

„Kunden“ gibt es immer genug!

Shadow