www.compliance-berater.de

Compliance Berater

CB

4 / 2019

Betriebs-Berater Compliance

27.3.2019 | 7.Jg
Seiten 93–136

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

CB-BEITRAG

Holger Ahrend

Cyberangriffe in der Realität

Cybersicherheit – ein großer Begriff im Jahr 2019. Aber was genau steckt eigentlich dahinter? Manche betrachten Cybersicherheit als Synonym für IT-Security-Compliance, also der Einhaltung anerkannter Standards wie der ISO 27001 oder dem BSI Grundschutzkatalog. Ist der Compliance-Audit bestanden und das Zertifikat erteilt, sollte man als Unternehmen vor Hackern geschützt sein – könnte man meinen. Die Realität sieht allerdings anders aus – denn gute Vorgaben, Dokumentationen und unterzeichnete Risikoübernahmen halten Angreifer leider nicht aus dem Netzwerk fern. Um sich abseits der Compliance also tatsächlich zu schützen, braucht es technische Expertise und ein solide aufgestelltes IT-System. Der Beitrag beschreibt auch für „Nicht-ITler" verständlich, welche Angriffswege genutzt werden und wie Unternehmen sich dagegen schützen können.

I. Warum und von wem werden Sie angegriffen?

Zunächst einmal muss man sich bewusst sein, mit wem man es da draußen eigentlich zu tun hat. Wer sind also diese Hacker, die jeden Tag private, gewerbliche oder sogar staatliche Netzwerke angreifen. Und welche Techniken nutzen sie, um bei Firmen oder Behörden einzusteigen? Grob kann man Angreifer in drei verschiedene Kategorien einsortieren:

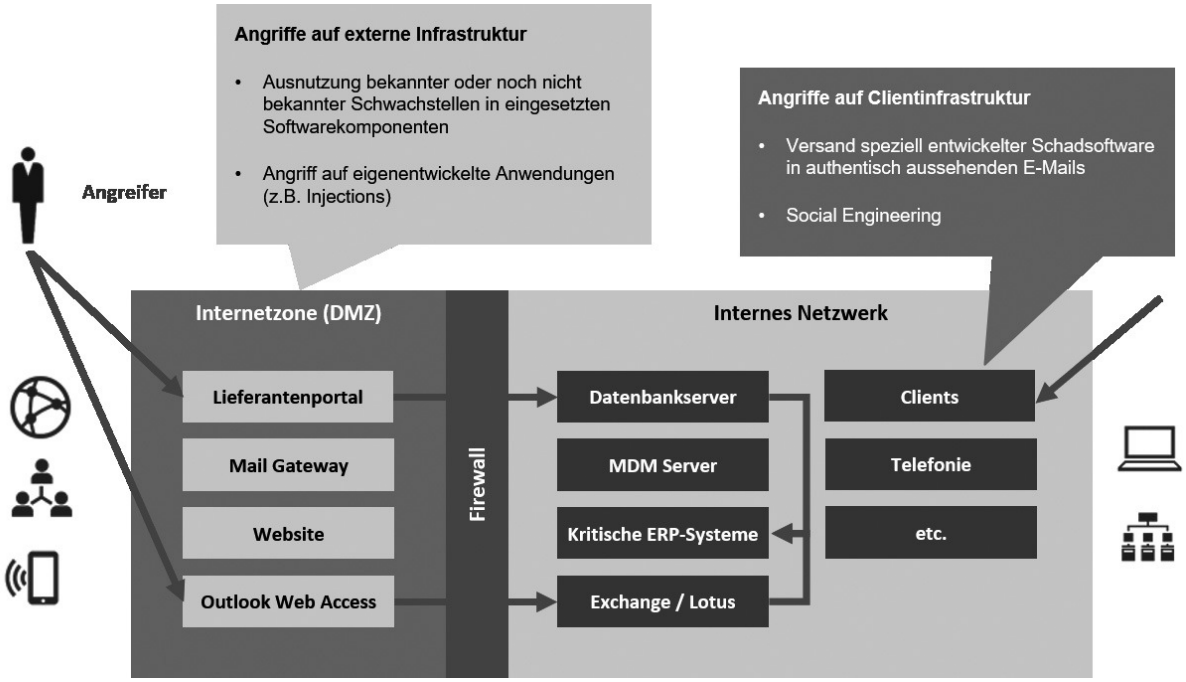
- Den Internetkriminellen – dieser hat nicht konkret Ihr Unternehmen im Auge. Ihm geht es vielmehr darum, dass er für seine kriminellen Machenschaften Systeme übernimmt, auf denen er diese ausüben kann. Der Internetkriminelle übernimmt somit Ihr E-Mail System, um Spam zu versenden oder Ihre Website, um darauf Schadsoftware wie Erpressungstrojaner zu verteilen. Dazu bedient er sich meist einfacher Techniken – er scannt jeden Tag das Internet nach verwundbaren Systemen und nutzt dann beispielsweise offensichtliche Konfigurationslücken oder nicht mit Sicherheitsupdates versorgte Systeme. Tiefer wird er eher nicht in Ihr Netzwerk einstiegen – dennoch kann ein solcher Angriff unschöne Auswirkungen auf die Reputation Ihres Unternehmens nach sich ziehen.
- Den Hacktivisten – dieser Angreifer ist eher politisch motiviert und hat es auf Unternehmen abgesehen, die nicht in sein Weltbild passen. Betroffen sind von dieser Gruppe meist Pharmaunternehmen, die Rüstungsindustrie oder Finanzinstitute. Auch hier sind die Angriffstechniken eher unspektakulär – dem Hacktivisten geht es meist darum, Schaden durch Systemausfälle zu erzeugen. Er beschießt Ihre Systeme einfach so lange mit sinnlosen Netzwerkanfragen, bis diese unter der Last zusammenbrechen.
- Zu guter Letzt kommen wir noch zu den gefährlichsten Angreifern – den gezielten. Darunter versteht man Hacker, die es konkret und ausschließlich auf Ihr Unternehmen abgesehen haben. Diese sind deshalb so gefährlich, weil sie meist weder Zeit noch Geld (im Rahmen ihrer individuellen Möglichkeiten) scheuen, um an ihr Ziel zu gelangen. Die Techniken sind ausgefeilt, vielfältig und mitunter unberechenbar. Zu dieser Kategorie von Angreifern gehören meist ehemalige, verärgerte Mitarbeiter, Kunden oder andere Personen, die mit Ihrem Unternehmen schädliche Erfahrungen gemacht haben. Aber auch Internetkriminelle können zu motivierten Angreifern werden, wenn sie bemerken, dass sich mit wenig Aufwand viele Informationen aus Ihrem Netzwerk entwenden lassen.

Diese dritte Kategorie von Angreifern wird besonders dann gefährlich, wenn Insiderwissen vorhanden ist. Das erleichtert ihnen den Weg durch das Netzwerk, da gegebenenfalls Schwachpunkte oder, noch schlimmer, alte Passwörter bekannt sind. Bemerkt werden diese Angreifer meist erst dann, wenn es schon zu spät ist – wenn die Daten bereits das Netzwerk verlassen haben. Darum widmet sich dieser Beitrag hauptsächlich diesen Angriffen.

II. Wie kommt der Angreifer in Ihr Netzwerk?

Aller Anfang ist schwer – und das gilt natürlich auch für den Hacker, der in Ihr Netzwerk möchte. Zunächst einmal braucht es einen initialen Weg in die IT-Systeme eines Unternehmens. Daher beginnt auch der gezielte Angreifer zunächst einmal damit, Ihre Systeme aus dem Internet zu begutachten. Er wird herausfinden, welche Dienste Sie nach außen anbieten – dazu zählen beispielsweise Lieferantenportale, E-Mail Systeme oder die Unternehmenswebsite. Besonderer Wert wird auf Schwachstellen gelegt, die sich dazu eignen, möglichst sofort und ohne Umwege eigene Befehle (Code) auf Ihren Systemen auszuführen. Ein Beispiel für eine derartige Sicherheitslücke ist „Eternal Blue". Die Lücke sorgte im Frühjahr 2017 für Furore, als sich darüber die Erpressungstrojaner „WannaCry" und „NotPetya" verbreiteten und große Unternehmen wie Maersk für Wochen lahmlegten (im Übrigen ein Beispiel für einen Angriff durch einen Internetkriminellen). Oft werden auch selbst entwickelte Lösungen wie Kundenportale als Einstiegspunkt verwendet. Da diese teilweise historisch gewachsen sind und nie auf sicheres Design betrachtet wurden, finden gewitzte Angreifer hier oft und sehr schnell die passende Schwachstelle.

Abb.: Illustration der Angriffswege



Klappt der Angriff, so hat der Hacker seinen ersten Schritt in das Netzwerk gemacht. Klappt er nicht, so wird der nächste Einstiegspunkt gesucht – und das sind meist die Computer der Anwender. Es gilt dann, die Schwachstelle Mensch zu nutzen, um sich einen Weg in die IT-Systeme zu erschleichen – man spricht bei solchen Techniken von Social Engineering. Eine beliebte Technik ist hier beispielsweise der Versand von Phishing-Mails, die von echten internen Unternehmens E-Mails nur sehr schwer zu unterscheiden sind. Besonders beliebt und in der Realität schon oft gesehen sind angebliche Warnnachrichten des E-Mail-Servers, dass das Postfach fast voll sei und man sich schnellstmöglich zur Onlinearchivierung anmelden solle. Auf den Link geklickt erscheint eine täuschend echte Loginseite zum Web-E-Mail-System des Unternehmens. Gibt man sein Passwort ein, hat man dem Angreifer genau das geliefert, was er sucht.

Eine weitere Methode ist der Versand schadhafter Dateianhänge. Besonders beliebt sind hier beispielsweise PDF-Dokumente, die es auf Schwachstellen in den jeweiligen Betrachtungsprogrammen abgesehen haben oder Microsoft Office-Dokumente mit Makros, die als Bewerbung oder Rechnung getarnt sind. Die Erfolgsquote solcher Angriffe ist leider erschreckend hoch, und während Antivirensysteme bekannte Angriffswellen oft zuverlässig erkennen, so scheitern sie meist bei der Erkennung von individuell entwickelter Schadsoftware eines gezielten Angreifers.

Ist auch der Erstangriff durch diese Techniken nicht erfolgreich, folgt der physische Gebäudezugang. Dabei muss der Angreifer nicht zwingend richtig in Ihre Firma einbrechen. Das „versehentliche" Verlieren eines schadhaften USB-Sticks vor dem Eingang reicht unter Umständen völlig aus, um die menschliche Neugierde zu triggern und Mitarbeiter dazu zu bringen, diesen in ihr Firmengerät zu stecken. Auch gibt es heute raffinierte Geräte in der Größe eines USB-Sticks, die in eine Netzwerkdose in Ihrem öffentlich zugänglichen Meeting- oder Schulungsbereich gesteckt werden und per Mobilfunk den Fernzugang in Ihr Netzwerk freimachen. Bemerkt werden diese meist erst dann, wenn es bereits zu spät ist.

III. Im Netzwerk angekommen – was nun?

Ist der Angreifer, beispielsweise durch eine der oben beschriebenen Methoden, in Ihr Netzwerk eingedrungen, passiert meist für drei bis sechs Monate gar nichts mehr. Warum? Weil der Angreifer sich sicher sein möchte, dass der Erstzugriff unerkannt geblieben ist. Meist werden in regelmäßigen Monatsabständen alte Protokolldateien überschrieben, so dass der Erstzugriff zu diesem Zeitpunkt nicht mehr nachvollziehbar ist.

Sobald er sich auf sicherem Terrain fühlt, beginnt er damit, sich weiter in Ihrem Netzwerk auszubreiten. Der erste Schritt ist meist das Sichern des Zugriffspunktes für den Fall, dass die initial ausgenutzte Schwachstelle behoben wird. Hierzu wird meist eine so genannte Shell installiert. Dabei handelt es sich um sehr kleine Programme für den unautorisierten Fernzugriff, deren genaue Funktionsweise und Unterbringung nur der Angreifer kennt. Antivirenprogramme scheitern meist bei deren Erkennung, sofern diese nicht durch besonders auffälliges Verhalten wie sehr große Uploads auf sich aufmerksam machen. Bei einem Kunden konnte ich beispielsweise eine Datei ermitteln, die sich als regulärer Windows-Web-Dienst getarnt hatte. Aufgefallen ist die Datei nur, weil das Erstellungsdatum und die Größe nicht zur legitimen Datei passten. Genauere Analysen zeigten dann, dass der Dienst dafür genutzt werden konnte, durch die Website des Unternehmens zu anderen internen Diensten, z. B. Benutzerlaufwerken, zu tunneln.

Ist der Zugang erst einmal gesichert, steht die Erweiterung der aktuellen Benutzerrechte auf dem Programm: Hat der Angreifer das Konto eines normalen Anwenders übernommen, so braucht er nunmehr administrative Berechtigungen, um sich weiter zu hangeln. Um an diese zu gelangen gibt es verschiedenste Techniken. Die relevantesten hierbei sind:

- die Ausnutzung einer Schwachstelle im Betriebssystem des übernommenen Computers,

- die Übernahme eines Dienstes, der mit sehr hohen Berechtigungen arbeitet (beispielsweise ein Backupdienst, der alle Abteilungslaufwerke sichert),
- das Auslesen administrativer Passwörter aus ungeschützten Konfigurationseinstellungen, in denen diese im Klartext vorliegen,
- das Mitlesen von internem Netzwerk- oder WLAN-Datenverkehr, um so durch unverschlüsselte Übertragungen direkt an das Passwort eines Administrators zu gelangen (hierzu braucht es natürlich passende Programme, die erst auf dem Rechner platziert werden müssen – dies ist daher ein eher selten gewählter Weg).

Verfügt der Angreifer erst einmal über administrative Berechtigungen auf dem übernommenen System, wird er zunächst seine bei der Rechteerweiterung erzeugten Spuren verwischen, also die Protokolldateien bereinigen. Das ist mit entsprechenden Berechtigungen nicht schwer und schnell erledigt, erschwert jedoch die Suche nach verwertbarem Material bei einer forensischen Angriffsuntersuchung. Ein speziell abgesicherter Server, der die Protokolldaten aller Systeme sicher sammelt und aufbewahrt, fehlt leider in den meisten Unternehmen, weshalb sich die Rekonstruktion von Angriffen im Nachhinein oft schwierig gestaltet.

Durch die erhöhten Berechtigungen gelangt der Angreifer nun an kritische Systemdaten – beispielsweise an die verschlüsselten Passwörter oder die Zertifikate der anderen Anwender des gekaperten Systems.

IV. Jemand hat mein Passwort geknackt

Um die verschlüsselten Passwörter nun zu knacken und wieder in passenden Klartext umzurechnen, kommen so genannte Password-Cracking-Angriffe zum Einsatz. Um diese zu verstehen, benötigt es einen kleinen Ausflug in die Passwortsicherheit.

Die meisten Unternehmen haben heutzutage die normalen, als sicher angesehenen und von Compliance-Auditoren gerne als gut abgehakten Passwortregeln: alle 30-90 Tage muss der Anwender sein Passwort ändern, mindestens 8 Zeichen müssen es sein, Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen müssen natürlich ebenfalls enthalten sein. Die Illusion, dass diese Regelung zur hohen und ausreichenden Passwortsicherheit führt, ist leider weit verbreitet. Mit Passwörtern hält es sich aber wie mit vielen anderen Dingen im Leben – das richtige Maß ist entscheidend. Macht man die Passwortregeln zu lasch, nutzen die Anwender Passwörter wie „qwertz“ oder „123456“. Übertreibt man es, werden die Passwörter als Zettel an den Bildschirm geklebt oder in Textdateien auf dem Desktop hinterlegt. Auch der ständige Zwang zur Änderung führt dazu, dass Anwender meist einfach nur durchzählen (Frankfurt!1, Frankfurt!2, …).

Ein Passwort, das die oben genannten Kriterien erfüllt, muss also nicht zwingend gut sein. Und hat man ein wirklich sicheres Passwort gewählt, dann müsste man es eigentlich auch nicht nach 30 Tagen wieder ändern. Der Schlüssel zu einem wirklich guten Passwort ist, keine Wörter zu nutzen, die im Wörterbuch stehen. Denn genau diese Wörterbücher nutzen Angreifer für sich, um so genannte Hybridangriffe durchzuführen. Dabei werden Wörter aus dem Wörterbuch in Kombination mit anderen Zeichen durchprobiert. Um auf das oben genannte Beispiel zu kommen, probieren die speziellen Password-Cracking Programme das Wort „Frankfurt“ und im Anschluss „Frankfurt1“, „Frankfurt$1“ und „Frankfurt!1“ aus. Derartige Programme gibt es jedoch nicht teuer auf dem Schwarzmarkt zu kaufen, sondern sind öffentlich und kostenlos im Internet für jedermann verfügbar. Die Erfolgsquote solcher Angriffe ist leider sehr hoch, weshalb eine entsprechende Schulung der Mitarbeiter zur Erstellung wirklich sicherer Passwörter sinnvoller wäre, als der heute überall durchgesetzte Änderungszwang.

V. Das Passwort ist unknackbar

Ist der Angreifer nicht in der Lage, die erbeuteten verschlüsselten Passwörter wieder in Klartext umzuwandeln, muss er sich anderer Techniken bedienen. Sofern das Passwort nicht zufällig in einer Textdatei im Klartext abgelegt wurde (was in der Realität leider auch sehr oft vorkommt), muss der Angriff also anders durchgeführt werden. Hierzu gibt es bekannte Angriffsverfahren, bei denen der Angreifer nicht das eigentliche Passwort, sondern lediglich das verschlüsselte benötigt. Die genauen technischen Details derartiger Angriffe würden den Rahmen dieses Artikels sprengen – jedoch sei so viel gesagt, dass derartige Verfahren durchaus ebenso verbreitet sind und genutzt werden. Die dafür benötigten Programme sind, Sie ahnen es, auch öffentlich verfügbar. Sie sind jedoch mit Einschränkungen verbunden. Ein Angreifer wird also immer versuchen, an das Klartextpasswort zu gelangen.

Bleibt dem Angreifer gar kein anderer Weg mehr, greift er zu anderen Methoden, um sich weiter durch das Netzwerk zu arbeiten. Hierzu wird der Fokus auf technisch besonders kritische, meist nur intern erreichbare Systeme gelegt. Ein aktuelles und brisantes Beispiel liefert der Microsoft Exchange Server. Dieser ist in den meisten Unternehmen im Einsatz – er liefert E-Mails, Kalender, Kontakte und Aufgaben in Outlook und erlaubt die Synchronisierung zu mobilen Geräten. Für Exchange wurde kürzlich eine schwere Sicherheitslücke bekannt, die es unter Umständen erlaubte, aus einem normalen Benutzerkonto eines mit den höchstmöglichen Berechtigungen zu machen. Für diese Schwachstelle gab es zwei Wochen lang kein passendes Sicherheitsupdate, wodurch Unternehmen weltweit gefährdet waren. Da der gezielte Angreifer wie eingangs erwähnt keinen Zeitdruck hat, wartet er unter Umständen auf genau diesen Moment, um seine Berechtigungen auf das gewünschte Level anzuheben. Und da Gelegenheit bekanntlich Diebe macht, ist man als Unternehmen auch nicht davor sicher, dass ein sowieso schon frustrierter Mitarbeiter nicht genau in diesem Moment zuschlägt.

VI. Weiter durchs interne Netzwerk

Hat der Angreifer genug Benutzerkonten gekapert, so wird er sich mit diesen ihm bekannten Zugangsdaten auf weitere Systeme verbinden. Ist er über ein direkt ans Internet angebundenes System, also beispielsweise ein Lieferantenportal (eine über das Internet erreichbare Website zur Kommunikation mit externen Dienstleistern), ins Netzwerk gelangt, so muss er unter Umständen noch die Barriere zwischen den Internetsystemen und dem internen Netzwerk überwinden. Hierzu macht er sich meist Systeme zu Nutze, die Anbindungen in das interne Netzwerk haben. Ein prominentes Beispiel sind auch hier wieder die Lieferantenportale: oft werden die tatsächlichen Daten nicht in der Internetzone (einem speziell gesicherten Bereich zwischen dem Internet und dem internen Firmennetzwerk), sondern direkt im internen Netz aufbewahrt. Damit das Portal auf diese Daten zugreifen kann, wird ein entsprechendes Loch in die Firewall gebohrt,

so dass das Internetsystem eine Verbindung zur internen Datenbank herstellen kann.

Der Angreifer, der auf den Internetsystemen bereits zu Hause ist, sucht sich genau solche Verbindungen und nutzt diese, um sich weiter ins interne Netzwerk zu befördern. Gerade bei Datenbankanbindungen werden oft handwerkliche Fehler gemacht – meist sind die technischen Benutzerkonten, die hierzu auf der Datenbank angelegt werden, mit zu hohen Berechtigungen ausgestattet. Auch beliebt ist das direkte Eintragen des Administratorkontos für die Datenbank zur Herstellung der Verbindung. Nutzt ein Angreifer dieses Konto, so kann er die Datenbank aufgrund der zu hohen Berechtigungen anweisen, seine ganz eigenen Befehle auf dem internen Server umzusetzen. Meist wird dies genutzt, um eine weitere Shell auf dem betroffenen System unterzubringen. Durch diese gelangt der Angreifer dann durch zwei Tunnel auf die kritischen Systeme, die eigentlich nur dann erreichbar sein sollten, wenn man sich auch physisch in der Firma befindet. Derartige Shells arbeiten träge und die Verbindungen zu den internen Systemen sind dadurch teilweise sehr langsam. Der gezielte Angreifer hat zwar viel Zeit, dennoch wird er auch hier wieder versuchen, sich eine dauerhafte Hintertür zu legen, die möglichst flotter läuft.

Und hier landet man letztendlich dann auch bei einem der letzten Schritte des Angreifers: der Schaffung von Wegen nach draußen, um die erfolgreiche Extraktion von Daten durchzuführen. Meist dient dieser Schritt sowohl der Beschleunigung des Zugriffs als auch dem Transport von Informationen aus dem Netzwerk. Um dieses Ziel zu erreichen, werden mitunter völlig harmlose Netzwerktechnologien durch den Angreifer zweckentfremdet. Ein Beispiel hierfür ist das so genannte Domain Name System (DNS). Sein eigentlicher Einsatzzweck ist es, Domänennamen (z. B. google.de) in die Netzwerkadresse des zu kontaktierenden Systems zu übersetzen, um die entsprechende Website für den Benutzer erreichbar zu machen. Die Technologie ist sehr alt und geht auf den Anfang der 80er Jahre zurück (wie auch die meisten anderen Basis-Netzwerkdienste). Zu dieser Zeit hatte sich noch niemand Gedanken über Cybersicherheit gemacht, weshalb diese Technologie anfällig für Missbrauch in verschiedensten Formen ist. Da Mitarbeiter im Internet arbeiten wollen (und sollen), ist DNS meist an den Firewalls von Unternehmen komplett nach außen freigeschaltet, und dadurch prädestiniert für einen Missbrauch zur Datenextraktion und Fernzugriff. Der Angreifer kapselt dabei die Daten in legitim aussehenden DNS-Datenverkehr, so dass die Firewall diesen einfach durchwinkt ohne ihn weiter zu hinterfragen.

Einige Unternehmen setzen heute jedoch so genannte „Next Generation Firewalls“ ein. Diese können nicht nur entscheiden, ob DNS erlaubt ist oder nicht, sondern prüfen auch, ob der dazugehörige Datenverkehr wirklich zu DNS passt. Derartige Firewalls können dann Alarm schlagen, wenn sich ein Hacker einer solchen Technik bedient. Daher missbrauchen Angreifer natürlich auch andere Technologien, um Daten möglichst verschlüsselt aus dem Netzwerk zu befördern. In der Realität konnte ich bereits einen Angriff beobachten, in dem der Angreifer die Daten einfach durch eine Art Browser auf einen Cloudspeicher geladen hat. Die Firewall betrachtete auch das als legitim, da Mitarbeiter ja die gleiche Netzwerktechnologie zum Surfen im Internet verwenden.

Zusammenfassend kann also gesagt werden, dass die Extraktion von Daten oft sehr schwer nachzuvollziehen ist. Und auch eine der erwähnten „Next Generation Firewalls“ hilft hier oft nicht weiter – denn wenn es bemerkt wird, ist der Angreifer meist bereits so tief im Netzwerk, dass es sowieso schon zu spät ist.

VII. Sicherheit? Warum, es ist doch noch nie etwas passiert!

Es ist also sehr schwer, einen gezielten Angreifer mit tiefem technischem Know-how aus dem eigenen Netzwerk fernzuhalten und / oder wirksam zu erkennen. Dennoch fahren heutzutage viele Firmen nach wie vor das Paradigma, in Sicherheit nicht zu viel Geld zu investieren, da ja noch nie etwas passiert sei. Ob sich nicht vielleicht ein Angreifer bereits im Netzwerk breit gemacht hat und nur auf den richtigen Moment wartet, die passenden Daten zu extrahieren, ist natürlich unbekannt, da aufgrund der fehlenden Investitionen die Überwachung eher einem Blindflug gleicht.

Doch nicht nur fehlende, sondern auch falsche Investitionen sorgen in vielen Unternehmen für mangelnde Cybersicherheit. Vor Kurzem habe ich ein Unternehmen beraten, das noch stellenweise das längst nicht mehr mit Sicherheitsupdates versorgte Windows XP im Einsatz hatte. Der Plan war dann, eine große Summe in ein so genanntes Instrusion Detection System – also ein System, das Angriffe erkennen soll – zu investieren. Dass Prävention immer den Fokus vor Detektion haben sollte und dass die Abschaltung uralter und stark verwundbarer Systeme mehr Sicherheit schafft als ein System, das erst Alarm schlägt, wenn es eigentlich zu spät ist, wollte niemand hören.

VIII. Wie erhöht man die eigene Cybersicherheit?

Was also können Unternehmen heute tun, um sich tatsächlich wirksam gegen Cyberangriffe zu schützen?

Um diese Frage zu beantworten, sollte man zu den eingangs erwähnten Arten von Angreifern zurückkehren. Denn die unmotivierten Hacker machen in etwa 95% aller Angreifer aus. Durch einige sehr einfache Prinzipien kann man die Cybersicherheit bereits so weit steigern, dass man derartige Angreifer möglichst wirksam aus dem eigenen Netzwerk draußen hält:

- Inventarisierung: Der erste und wichtigste Punkt dieser Aufzählung – viele Unternehmen sind sich heute gar nicht bewusst, welche IT-Systeme sie alle im Einsatz haben und wie diese genau miteinander zusammenhängen. Eine gute Inventarisierung von Hard- und Software kann dabei helfen, das Risiko von Schwachstellen besser einzuschätzen, Fremdgeräte aus dem Netzwerk fernzuhalten und die nächsten vier Punkte wirksam zu erfüllen.
- Update / Patch Management: Nichts ist so anfällig für einen Hacker wie veraltete Software. Auf dem Markt gibt es eine Vielzahl so genannter Schwachstellenscanner, die ganze Netzwerke innerhalb kürzester Zeit auf veraltete Software und die zugehörigen Sicherheitslücken abgrasen. Derartige Software kann man sich im eigenen Netzwerk zu Nutze machen, um Schwachstellen zu identifizieren und durch entsprechende Updates abzustellen.
- Sichere Konfiguration: Um die IT sicher zu betreiben, macht es Sinn, für strategisch eingesetzte Kernsoftware (z. B. Betriebssysteme, Office-Produkte) einen Mindeststandard für die sichere Konfiguration zu etablieren.
- Berechtigungsvergabe nach Minimalprinzip: Mitarbeiter sollten stets nur über die Berechtigungen verfügen, die sie tatsächlich zur Ausführung ihrer Arbeit benötigen. Die Nutzung administrativer Benutzerkonten für normale Alltagsaufgaben sollte niemals das Mittel der Wahl sein. Auch unnötige Zugriffsberechtigungen auf eine Vielzahl von Abteilungslaufwerken sollten noch einmal überdacht werden.

– Backups: Es klingt so banal und wie eine alte Leier, aber viele Unternehmen scheitern bei der Umsetzung ordentlicher Backup-Pläne. Sich darüber bewusst zu sein, welche IT-Systeme kritisch für den Betrieb und das geistige Eigentum des Unternehmens sind, kann dabei helfen, Datensicherungen und Zielvorgaben zu deren Wiederherstellung passend zu definieren. Auch helfen sie bei der Abwehr der mittlerweile sehr häufig vorkommenden Erpressungstrojaner.

Sind diese fünf grundlegenden Punkte ordentlich umgesetzt, ist man als Unternehmen im Hinblick auf die Cybersicherheit bereits besser aufgestellt als die meisten anderen und hat sich das Geld für die allseits beliebte ISO 27001 Zertifizierung dabei gespart.

Die Sinnhaftigkeit internationaler Standards wie der ISO 27001 soll mit diesen Worten natürlich nicht in Abrede gestellt werden. Es handelt sich dabei um ein gutes Regelwerk, das, technisch und organisatorisch gut implementiert, ebenfalls ein hohes Cybersicherheitsniveau herstellt. Nur krankt es leider häufig genau an dieser besagten Implementierung, da der Fokus bei Zertifizierungen zu stark auf die Dokumente als auf die reale technische Umsetzung gelegt wird. Und so schützt das Hochglanzzertifikat an der Wand am Ende nicht davor, selbst Opfer eines erfolgreichen Angriffs zu werden – was sich auch in von mir durchgeführten forensischen Untersuchungen schon gezeigt hat.

Langfristig betrachtet kann sich ein Unternehmen somit nur wirklich vor Angriffen schützen, indem die IT-Systeme tatsächlich technisch gegen Hacker gehärtet werden. Auch die Herstellung einer wirksamen technischen Überwachung durch so genannte Security Incident und Event Management (SIEM) Systeme kann helfen, Hacker bereits an der Vordertür zu stoppen.

Jedoch braucht es dafür technisches Fachwissen anstelle von Word-Dokumenten und Excel-Tabellen. Ansonsten läuft man als Unternehmen erhöhte Gefahr, sich in die Liste von Unternehmen wie Maersk, Equifax und Starwood einzureihen, die bis heute mit den Folgen erfolgreicher Hackerangriffe zu kämpfen haben.

IX. Cybersicherheit und Datenschutz

Zum Abschluss sollte man auch noch einen Bogen zum Datenschutz spannen, wenngleich diese Themen meist komplett voneinander getrennt betrachtet werden. Denn spätestens seit der Einführung der EU-DSGVO besteht für Unternehmen nicht nur das Risiko eines Reputationsschadens, sondern es drohen auch empfindliche Strafen im Hinblick auf Datenschutzverstöße, sollte ein Hacker erfolgreich die eigenen Kundendaten entwenden. Die Strafen sind dabei keine Peanuts – hier werden je nach Schwere des Verstoßes bis zu 4% des Jahresumsatzes durch die Behörden eingefordert. Der Vorstand bzw. die Geschäftsführung haftet dabei persönlich auch mit dem Privatvermögen, weshalb das Thema Cybersicherheit weit oben auf der Agenda von CEOs stehen sollte.

AUTOR

Holger Ahrend *ist unabhängiger Cyber Security Berater. Er hat mehr als 10 Jahre Erfahrung in der IT sowie über 7 Jahre Erfahrung in Security-Projekten. Durch seine beruflichen Stationen bei Deloitte, KPMG und Accenture hat er abseits der tiefen technischen IT-Expertise das notwendige Wissen über konzernrelevante Geschäftsprozesse. Er berät Unternehmen ganzheitlich bei der Prävention und Erkennung von Cyber-Vorfällen.*

Compliance-Berater Zitierweise CB: / ISSN 2195-6685

CHEFREDAKTION:
Dr. Malte Passarge (V.i. S. d.P.), Passarge, Prudentino & Rhein Rechtsanwälte PartGmbB – Studio Legale, Große Johannisstraße 19, 20 457 Hamburg, Tel: 040-4 14 25 51-0, passarge@ppr-recht.de

REDAKTION:
Christina Kahlen-Pappas, Tel. 0151-27 24 56 63, christina.kahlen-pappas@dfv.de

HERAUSGEBER:
Prof. Dr. Frank Beine, WP/StB
Hanno Hinzmann
Manuela Mackert
Dr. Philip Matthey
Univ.-Prof. Dr. Annemarie Matusche-Beckmann
Dr. Dirk Christoph Schautes
Prof. Dr. Martin Schulz, LL.M. (Yale)
Eric S. Soong
Prof. Dr. Gregor Thüsing, LL.M. (Harvard), Attorney at law (New York)
Dr. Martin Wienke

BEIRAT:
Dr. Martin Auer
Dr. Martin Bünning, RA/StB
Dr. José Campos Nave, RA/FAHaGesR/FAStR
Dr. Peter Christ, RA/FAArbR
Dr. Susanne Jochheim, RAin
Dr. Ulf Klebeck, RA
Tobias Neufeld, LL.M. (London), RA/FAArbR, Solicitor (England & Wales)
Jürgen Pauthner, LL.M. (San Diego), MBA
Mario Prudentino, RA
Dr. Manfred Rack, RA
Dr. Sarah Reinhardt, RAin/FAArbR
Dr. Roman Reiß, RA/FAStR
Gunther A. Weiss, LL.M. (Yale), RA, Attorney at law (New York), Advokát (Praha)
Wolfgang Werths
Tim Wybitul, RA/FAArbR
Prof. Dr. Dr. Jörg Zehetner, RA

dfv Mediengruppe

VERLAG: Deutscher Fachverlag GmbH, Mainzer Landstr. 251, 60326 Frankfurt am Main, Tel. 069-7595-2788, Fax 069-7595-2780, Internet: www.dfv.de, verlag@betriebs-berater.de

GESCHÄFTSFÜHRUNG: Angela Wisken (Sprecherin), Peter Esser, Markus Gotta, Peter Kley, Holger Knapp, Sönke Reimers
AUFSICHTSRAT: Klaus Kottmeier, Andreas Lorch, Catrin Lorch, Peter Ruß
GESAMTVERLAGSLEITUNG FACHMEDIEN RECHT UND WIRTSCHAFT: RA Torsten Kutschke
Tel. 0 69-75 95-27 01, Torsten.Kutschke@dfv.de

REGISTERGERICHT: AG Frankfurt am Main, HRB 8501

BANKVERBINDUNG: Frankfurter Sparkasse, Frankfurt am Main, Kto.-Nr. 34 926 (BLZ 500 502 01)

In der dfv Mediengruppe, Fachmedien Recht und Wirtschaft, erscheinen außerdem folgende Fachzeitschriften: Betriebs-Berater (BB), Causa Sport (CASP), Recht der Internationalen Wirtschaft (RIW), Datenschutz-Berater (DSB), Der Steuerberater (StB), Europäisches Wirtschafts- und Steuerrecht (EWS), Kommunikation & Recht (K&R), Netzwirtschaften & Recht (N&R), Zeitschrift für Vergleichende Rechtswissenschaft (ZVglRWiss), Zeitschrift für das gesamte Handels- und Wirtschaftsrecht (ZHR), Recht der Finanzinstrumente (RdF), Wettbewerb in Recht und Praxis (WRP), Zeitschrift zum Innovations- und Technikrecht (InTeR), Zeitschrift für das gesamte Lebensmittelrecht (ZLR) und Zeitschrift für Umweltpolitik & Umweltrecht (ZfU), Zeitschrift für Wett- und Glücksspielrecht (ZfWG), Zeitschrift für Neues Energierecht (ZNER).

ANZEIGEN:
Lena Moneck, lena.moneck@dfv.de
Es gilt Preisliste Nr. 7.

Bereichsleitung Finanzen und Medienservices: Thomas Berner, Tel. 069/7595-1147

Leitung Produktion: Hans Dreier, Tel. 069/7595-2463

Leitung Logistik: Ilja Sauer, Tel. 069/7595-2201

VERTRIEB: Ayhan Simsek, Tel. 069-7595-2782, ayhan.simsek@dfv.de

ERSCHEINUNGSWEISE: monatlich. Nicht eingegangene Hefte können nur bis zu 10 Tage nach Erscheinen des nächstfolgenden Heftes kostenlos reklamiert werden.

BEZUGSPREISE: Jahresvorzugspreis (11 Ausgaben): 509 Euro inkl. Vesandkosten und MwSt., Sonderpreis für Studenten und Referendare: 140,– Euro. Beorderungsgebühr jährlich (fällt an bei Fremdzahler): 2 Euro netto. Preis des Einzelheftes: 51,95 Euro. Auslandspreise auf Anfrage. Rechnungslegung erfolgt jährlich. Die Abonnementgebühren sind im Voraus zahlbar. Der Abonnementvertrag ist auf unbestimmte Zeit geschlossen. Eine Kündigung ist jederzeit bis 3 Monate vor Ende des Bezugszeitraumes möglich. Liegt dem Verlag zu diesem Zeitpunkt keine Kündigung vor, verlängert sich das Abonnement automatisch um ein weiteres Jahr zum dann gültigen Jahrespreis, zahlbar im Voraus. Auslandspreise auf Anfrage. Die Zeitschrift und alle in ihr enthaltenen Beiträge und Abbildungen sind urheberrechtlich geschützt.

SATZ: DFV – inhouse production

DRUCK: medienhaus Plump GmbH, Rolandsecker Weg 33, 53 619 Rheinbreitbach

VORSCHAU CB 5/2019

Dr. Christian Schefold, RA
15 Jahre Compliance

Dr. Malte Passarge, RA
Haftungsrisiken bei richtiger Anwendung falscher Gesetze?

Tobias Grambow, RA
Täter einer Straftat oder Ordnungswidrigkeit mit arbeitsrechtlichem Bezug

Prof. Dr. Oliver Haag und **Maximilian Jantz**
Compliance im Personalwesen

BB 13/2019

WIRTSCHAFTSRECHT

Dr. Moritz Keller, RA, und **Dr. Sunny Kapoor**, RA
Climate Change Litigation – zivilrechtliche Haftung für Treibhausgasemissionen

STEUERRECHT

Prof. Dr. Angelika Dölker, MBA International Taxation
Anbindung der Schweiz an das Steuerrecht der EU: Kapitalverkehrsfreiheit, Freizügigkeitsabkommen, BEPS und Anti Tax Avoidance Package

Andreas Walter, RA, **Malte J. Mehrgardt** und **Lena Freiin von Bechtolsheim**
Mietgarantien im Steuerrecht

BILANZRECHT UND BETRIEBSWIRTSCHAFT

Ralf Bose, WP/StB, und **Dr. Thomas Lilienbecker**, WP/StB
Praktische Auslegungsfragen zur Begrenzung von Nichtprüfungsleistungen

ARBEITSRECHT

Dr. Sebastian Naber, RA, **Dr. Willem Schulte**, RA, und **Katharina Tisch**
Wie „gut" ist gut genug? – BB-Rechtsprechungsreport zu Arbeitszeugnissen 2017/2018