Aktualisierungsstand: Frank W. Holliday, 6.12.2017

WIE KANN SICH EIN UNTERNEHMEN GEGEN CYBERATTACKEN WEHREN?

Das ist wirklich eine Frage des Budgets. Jede Vernetzung birgt Risiken von außen und eine Gefahr eines erleichterten Know-how-Abflusses insbesondere auch von innen (dies vergessen leider viele)!

Gängige Vorgehensweise ist das Zwiebelschalen-Prinzip:

Schutzmaßnahmen am Perimeter (also an der Grenze nach außen) sind unabdingbar. Z.B. dort eine Next Generation Firewall einsetzen. Sie bietet eine Analysemöglichkeit des Datenstromes auf höherem Niveau (Anwendungsprotokoll-Ebene) inklusive der Möglichkeit einer automatisierten Detektion von Eindringversuchen bis hin zur automatisierten Abwehr der Attacke (IDS/ IPS).

Dahinter sollte eine spezielle Schutzzone (demilitarisierte Zone/ DMZ) eingerichtet sein, in der sich alle IT-Systeme (gehärtet und nur auf die notwendigsten Dienste und Konten beschränkt!) mit ihren Anwendungen (auf das Essentielle beschränkt!) befinden, die einen "direkten Draht" nach außen übers Internet bereitstellen müssen (z.B. Web-Server, Internet-Dienste-Server).

Diese Zone wird über eine weitere Firewall wiederum kontrolliert abgeschottet gegen die IT-Innereien Ihres Unternehmens (z.B. Ihre Datenbanken oder sensitiven Datenhaltungsserver Ihres Unternehmens). Sie können sich auch je nach Frage des Budgets noch weitere gestaffelte Zwiebelschalen inklusive Netzsegmentierungen leisten. Denken Sie daran, je mehr Staffelung Ihre Verteidigungsmaßnahmen in der Tiefe aufweisen umso schwerer hat es ein Eindringling (Attacker/ Penetrator) bis zu Ihrem heiligstem Inneren ("Ihre Kronjuwelen" / Critical Assets) vorzudringen und/ oder einen Abfluss von Informationen aus dem Inneren heraus unentdeckt werden zu lassen. Haben Sie dann Ihre Kronjuwelen auch noch verschlüsselt gehalten, haben Sie wieder eine weitere Schicht, die Zugriffe kontrollierbarer macht und damit noch besser schützt!

Aber, wie gesagt, das ist alles eine Frage des Budgets und vor allem einer vorgeschalteten sorgfältigen Risikoanalyse mit Identifikation und Einschätzung vorhandener Risiken und Ableitung adäquater Schutzmaßnahmen. Denn Informationen, die z.B. im Internet stehen, brauchen nun mal nicht mit dem Schutzbedarf abgesichert werden wie Ihre Kronjuwelen. Mit einer sauber hergestellten Wertabstufung Ihrer Informationen (Asset Classification) und darauf basierendem abgestimmtem Absicherungsaufwand können Sie richtig Geld sparen!

Unerlässlich sind weiterhin regelmäßige Schulungen Ihrer Mitarbeiter, die über die Risiken aus dem Cyberraum aufklären insbesondere auch ereignisgesteuert bei aktuell auftretenden, schwerwiegenden Bedrohungen (deshalb ist die Beobachtung der aktuellen Bedrohungslage von sehr entscheidender Bedeutung). Dadurch wird ein Risikobewusstsein aller Mitarbeiter herausgebildet und geschärft (sozusagen "die menschliche innere Firewall" Ihres Unternehmens!).

Weiterhin gilt es anhand von regelmäßigen Penetrationstests Ihre Absicherung auszutesten. Die dadurch ermittelten Sicherheitslücken bzw. Defizite gilt es sodann zu schließen und somit Ihr Abwehrvermögen gegenüber den jeweilig aktuellen Bedrohungen anzupassen und systemisch nach und nach zu steigern (Steigerung der Resilienz).

Es gibt auch Perimeter-lose Sicherheitskonzepte, bei denen ein Innen und Außen keine Rolle mehr spielt. Hier kommen verstärkt kryptographische Verfahren bis hin zu einer ganzen kryptographischen Infrastruktur (PKI) zum Zuge. Dabei werden die Kommunikationsbeziehungen zwischen den

Kommunikationspartnern genau je nach definierter Schutzbedürftigkeit angemessen absichert und die Verwahrung der Informationen in den End-Points wiederum je nach Schutzbedürftigkeit mehr oder weniger sicher ausgestaltet. Google hat so was schon durchdekliniert, schauen Sie mal unter dem Link: www.beyondcorp.com nach. Die zeigen, wie man sowas hinbekommt.

Wie gesagt alles eine Frage des Geldes und Ihrer Bereitschaft Risiken bei fehlenden Sicherheitsmaßnahmen zu übernehmen (Risikoappetit).

WAS BEINHALTET EIN CYBER-SICHERHEITSCHECK?

Das BSI (deutsche zentralnationale Behörde für Informationssicherheit) und das German Chapter der ISACA (internationale Vereinigung zur Informationssicherheit) haben dazu einen Leitfaden mit dem Titel 'Leitfaden Cyber-Sicherheits-Check' herausgegeben. Den kann ich empfehlen heranzuzuziehen. Siehe unter Link:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden-Cyber-Sicherheits-Check.html

IST EINE CYBERVERSICHERUNG SINNVOLL UND WELCHE SCHÄDEN SIND DURCH EINE CYBERVERSICHERUNG GEDECKT?

Grundsätzlich müssen in einem zyklischen mitunter auch ereignisgesteuerten Prozess Risiken erkannt, eingeschätzt und qualifiziert behandelt werden. Viele kennen das unter dem Stichwort IKS (internes Kontrollsystem).

Für die Risikobehandlung bietet sich eine Auswahl von vier Behandlungsweisen an:
a) durch Geschäftsprozess-Redesign das Risiko vermeiden (manchmal ein Königsweg)
b) durch Gegenmaßnahmen das Risiko vermindern bzw. begrenzen (das häufigste Verfahren)
c) durch eine Versicherung das Risiko abdecken (aber immaterielle Schäden,
z.B. einen Imageverlust, tragen Sie nach wie vor selbst!)
d) das Risiko als Restrisiko annehmen (das machen leider viele infolge mangelhafter Risikoanalyse unbewusst!).

Am Anfang muss daher stehen zu analysieren, was sind die Bedrohungen und Gefahren, denen wir hier speziell im Cyberraum ausgesetzt sind. Wie gehen wir gemäß dem Schema oben damit um. Machen Sie sich klar, je weniger Sie a) & b) Handlungen gegenüber dem Versicherer vorzuweisen haben, wird Ihre Versicherung teurer bis hin zu nicht versicherbar.

Den Überblick, welche Schäden (in der Regel nur materieller Schaden insbesondere hier auf das Kleingedruckte achten) konkret vom Versicherer zu welchem Preis abgedeckt werden, erhalten Sie am besten durch Einholung mehrerer Versicherer-Angebote. Seriöse Versicherer machen dazu durch einen von Ihnen zu beantwortenden stichhaltigen Fragenkatalog oder sogar mittels einer Auditierung eine überblicksartige Risikofeststellung als Grundlage für die Preisgestaltung).

Sehr gerne kann ich Sie beim Prozess der Risikoanalyse und der Auswahl eines geeigneten Versicherers unterstützen.

WIE ERSTELLT MAN EIN SICHERES PASSWORT UND WIE OFT SOLLTE ES GEÄNDERT WERDEN?

Da sicherere, benutzerfreundlichere Alternativen noch nicht so ganz überzeugend sind, ist die Passworthandhabung für Ihre Sicherheit und Ihr Risiko nach wie vor von entscheidender Bedeutung! Sie können ihre Sicherheit beträchtlich erhöhen in dieser Frage, wenn Sie für diese Art von Authentifizierung (Echtheitsprüfung der Person) zusätzlich noch andere Faktoren einsetzen. Man spricht dann von einer Mehr-Faktoren-Authentifizierung MFA oder bei zwei Methoden von 2FA. Eine schöne Beschreibung zur 2FA finden Sie übrigens in Wikipedia unter dem Link:

https://de.wikipedia.org/wiki/Zwei-Faktor-Authentifizierung

Prinzipiell gilt je länger die Passwörter sind umso sicherer werden Sie unknackbar. Mit jeder Zeichenstelle mehr wächst der Permutationsbaum nach und nach exponentiell. Was sich im logarithmischen Maßstab der Passwortentropie - in bits angegeben - in einem linearen Anstieg darstellt. Ein Beispiel: eine Entropie von 40 bits entspricht einem Permutationsbaum von 2 hoch 40 Elementen. Eine Entropie von 80 bits entspricht schon einem Permutationsbaum von 2 hoch 40 **mal** 2 hoch 40 Elementen! Legen Sie den alphabetischen Kleinbuchstabenzeichensatz zugrunde mit 25 Zeichen dann erhalten Sie 40 bits Entropie durch eine Zeichenlänge von aufgerundet 9 Stellen. Eine Entropie von 80 bits (und diese Entropie ist schon nicht schlecht!) erhalten Sie dann in etwa durch die doppelte Zeichenlänge von 18 Stellen. Sie sehen schon durch 18 Stellen von Kleinbuchstaben kann man eine ordentliche Entropie erzeugen.

Anwendung: Bilden Sie einen langen Merksatz. Verketten Sie alle Wörter in Kleinbuchstaben geschrieben hintereinander, und Sie müssen dabei nicht einmal die Shift-Taste drücken;-). Bei einem ordentlich langen Merksatz versammeln Sie Zeichenstellen nur noch so dahin und Sie haben im Nu eine bombastische Passwortentropie!

Kleiner Tipp dazu: Setzen Sie einen Passwort-Safe oder -manager ein, damit Sie gut unterstützt für jeden Zugang - und das ist für Ihr Risiko wichtig! - tatsächlich ein eigenes Passwort definieren. Nehmen Sie zum Beispiel den kostenlosen Passwort-Safe 'KeePass' (beziehbar über den Link: https://keepass.info/ und das https ist für Ihre Sicherheit wichtig!). Der ist sogar für viele verschiedenartige Betriebssysteme erhältlich (Interoperabilität) und zeigt Ihnen gleich die Passwortentropie in bits angegeben mit an. Immerhin ist die Datenhaltung dieses Passwortmanagers ab Version 2 mit AES-256bit verschlüsselt. Selbst Quantencomputer der chinesischen oder amerikanischen Dienste können da nicht ran:-) Kombinieren Sie das jetzt für die die Ablage mit einer abgesicherten Private-Cloud, haben Sie den sogar weltweit unter Anwendung einer verschlüsselten VPN-Verbindung per Internet sicher bei sich zur Verfügung! Ganz Mutige legen die Datenhaltung von KeePass gleich z.B. in DropBox ab.

Bei nach obigem Verfahren so leicht erzeugten großen Passwortlängen können Sie sich es leisten, den nervig häufigen gerade auch sehr mit Sicherheitsproblemen verbundenen Passwortwechsel zu sparen. Jährliche Perioden sind dann voll ausreichend, wenn Sie mehr Risikoappetit und Passwortentropien >= 128 bits haben, können Sie es riskieren es gleich ganz sein zu lassen. Sie tragen dann allerdings das Risiko einer unentdeckt gebliebenen Kompromittierung des Passworts, welches Sie durch die regelmäßigen Passwortwechsel als Gegenmaßnahme minimieren (mitigieren) oder noch besser durch eine Zwei-Faktoren-Authentifizierung (2FA), z.B. insbesondere für den

Masterpasswortzugang eines Passwort-Safes, kompensieren. Wird ein Passwort "abgephisht" (leider nach wie vor eine weltweit erfolgreiche Methode!) oder das Passwort wird versehentlich, wenn nicht sogar absichtlich, oder durch die gelungene Platzierung eines Keyloggers zugänglich gemacht (Kompromittierung), dann müssen Sie so schnell wie möglich handeln und das Passwort auswechseln (so in etwa lautet auch die neueste Empfehlung der amerikanischen Standardorganisation NIST).

Besonderes Augenmerk gilt es den voreingestellten Passwörtern von Herstellern zu widmen. Den Hackern sind diese so gut wie alle bekannt! Hier gilt es unbedingt auf alle Fälle das voreingestellte Passwort durch ein eigen definiertes sicheres Passwort so rasch wie möglich auszutauschen. Sie glauben nicht, was diese Sicherheitslücke sogar bei größeren (oder gerade deswegen?) Unternehmen an enormen Schäden auslösen kann.

Um das Ganze noch näher zu beleuchten kann ich den Leitfaden des BSI empfehlen unter dem Link:

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

Vergessen Sie aber den Quatsch mit den vielen einzusetzenden Zeichenklassen. Das kommt noch aus den Zeiten als Passwörter höchstens 8 oder noch weniger Stellen aufweisen durften um damit noch einen Hauch von Entropie erzeugen zu können. Aber mit den obigen Ausführungen verstehen Sie das jetzt ja: Der bedeutend entscheidendere Treiber für Ihre Passwortsicherheit ist der Einsatz großer Passwortlängen.

Eine sehr gute Referenz zum Wissen über Passwörter finden Sie in Wikipedia unter dem Link:

https://de.wikipedia.org/wiki/Passwort

Dem gibt es dann nichts mehr an Wissen hinzuzufügen.

WAS MUSS ICH BEZÜGLICH DER SICHERHEIT VON PASSWÖRTERN BEACHTEN?

Hier gilt gleich zu Beginn die erteilte Antwort auf die vorherige Frage, also lesen Sie sich die Antwort auf die vorherige Frage ruhig mal durch.

Besonderes Augenmerk gilt es den voreingestellten Passwörtern von Herstellern zu widmen. Den Hackern sind diese so gut wie alle bekannt! Hier gilt es unbedingt auf alle Fälle das voreingestellte Passwort durch ein eigen definiertes sicheres Passwort so rasch wie möglich auszutauschen. Sie glauben nicht, was diese Sicherheitslücke sogar bei größeren (oder gerade deswegen?) Unternehmen an enormen Schäden auslösen kann.

Um das Ganze noch näher zu beleuchten kann ich den Leitfaden des BSI unter dem Link empfehlen:
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

Vergessen Sie aber den Quatsch mit den vielen einzusetzenden Zeichenklassen. Das kommt noch aus den Zeiten als Passwörter höchstens 8 oder noch weniger Stellen aufweisen durften um damit noch einen Hauch von Entropie erzeugen zu können. Mit den Ausführungen der Antwort auf die vorherige Frage verstehen Sie das ja: Der bedeutend entscheidendere Treiber für Ihre Passwortsicherheit ist der Einsatz großer Passwortlängen.

Wie in vorheriger Antwort gesagt: Eine sehr gute Referenz zum Wissen über Passwörter finden Sie in Wikipedia unter dem Link: https://de.wikipedia.org/wiki/Passwort

WIE SICHER SIND DATEN IN DER CLOUD?

Wie die Juristen so schön sagen: "Das Urteil hängt vom Einzelfall ab". Ein paar grundsätzliche Überlegungen gibt es aber schon.

Um was für eine Cloud-Lösung handelt es sich überhaupt:

- Ist es eine selbst unter voller eigener Kontrolle aufgebaute Cloud-Lösung im und fürs Unternehmen (*Private Cloud*).
- Ist es eine über einen Transportkanal (i.d.R. das Internet) unter Anbindung eines Cloud-Providers erfolgende reine Datenkommunikation (ausgelagerte nun mitunter weltweit zentral verfügbare Datenräume) oder gar eine komplette Prozessabwicklungskommunikation (BaaS), beispielsweise die Vertriebsbusiness-Lösung *salesforce* (*Public Cloud*).
- Oder ist es eine Mischform von beidem (*Hybride Cloud*).

Analysieren Sie sorgfältig was lohnt sich, für das Bereitstellen einer bestimmten IT-Basisinfrastruktur (IaaS), von geschickter zentraler Datenhaltung (PaaS) bis hin zur Auslagerung kompletter Geschäftsprozesse (SaaS oder gar BaaS) überhaupt einem Außenstehen (und das sind Cloud-Provider immer) unter welchen Risikobedingungen und Kostenvorstellungen in die Hand zu geben (Public Cloud) oder doch unter vollständiger eigener Kontrolle (Private Cloud) mittels der Cloud-Instrumentarien dem Unternehmen verfügbar zu machen, oder eine Mischform von beidem als zielführender anzustreben (Hybride Cloud).

Bei einer Public Cloud-Lösung übergeben Sie zwangsläufig die Kontrolle über Ihre ausgelagerten Informationswerte (Assets) teilweise in die Hände Ihres Cloud-Providers umso mehr sind Sie darauf angewiesen in einer Vertragsgestaltung mit dem Cloud-Provider dies zu kompensieren.

Ganz wichtig gilt es im Vertrag rechtliche Bedingungen zu regeln, z.B. die Zusicherung, dass die übergebenen Daten nur in einem bestimmten Rechtsraum allokiert werden, z.B. ausschließlich nur im EU-Raum oder nur in Deutschland.

Auch Sicherheitsaspekte gehören im Dienstleitungsvertrag festgezurrt geregelt, so u.a. festgelegte Vorkehrungen zur Gewährleistung der Vertraulichkeit, insbesondere beim Transport über das Internet, einer sichergestellten mandantenfähigen Datenhaltung beim Provider, zur Gewährleistung der Informationsintegrität, insbesondere verfälschungssichere, die Vollständigkeit wahrende Datenhaltung und nicht zu vergessen gerade im Hinblick auf die ab 25. Mai 2018 sanktionierbare EU-DSGVO Zusicherung einer mandantenfähigen Datensicherung, zur Gewährleistung der Verfügbarkeit, insbesondere zugesicherte Responsezeiten und Wiederanlauf-Zeiten, maximale Einzel-Ausfallzeit und maximale Summe von Ausfallzeiten eines Jahres. Regelungen zur Schutzbedürftigkeit und zu wirkenden Schutzmaßnahmen Ihrer dem Provider anvertrauten Assets gehören in den Vertrag oder sollten zumindest dort Regelungen vorsehen. Die Handhabung von Sicherheitsvorfällen beim Provider und seine Pflicht Sie darüber zu informieren und den entstandenen Schaden so gering wie möglich zu halten sind ein wichtiger Vertragspunkt. Wenn möglich sollten Sie hier eine Regress-Klausel durchsetzen.

Die Sicherstellung von Audit-Rechten beim Cloud-Provider sind wichtiger Vertragsgegenstand oder zumindest der Nachweis einer Auditierung oder einer Zertifizierung durch renommierte Dritte. Hat der Provider hier was zu bieten, so steigert es das Vertrauen in den Provider mit "Sicherheit".

Machen Sie sich klar, jeder getroffener, vertraglich abgesicherter Regelungspunkt (eben alles was Ihre Informationssicherheit und Ihre Geschäftskontinuität sicherstellt und steuert) hilft die Abgabe von Kontrolle Ihrer Assets an den Provider zu kompensieren.

Sie sollten auch nicht vergessen vertraglich Vorkehrungen zu treffen für die Möglichkeit eines Wieder-Insourcings oder für die Durchführbarkeit eines Cloud-Provider-Wechsels, was die Unabhängigkeit vom Provider deutlich erhöht.

Denken Sie immer daran je mehr Freiheiten Sie Ihrem Provider gönnen umso abhängiger werden Sie von ihm, was nachhaltig den Provider mehr und mehr zur Erhöhung des Preises "verführt".

Es gibt im deutschen Mittelstand sehr leistungsfähige Cloud-Provider, die insbesondere Ihre Sicherheitsanliegen kundenorientiert vertraglich aufnehmen.

Bei den großen amerikanischen Anbietern, wie Amazon, Google, HP, IBM oder Microsoft um mal ein paar zu nennen, bekommen Sie nur Verträge von der Stange, die sehr schwierig zu ändern sind. Das Angebot dieser großen Anbieter kommt zum Einstieg mit Leichtfüßigkeit da her und verführt - nicht zu unterschätzen - auch gerade viele Unternehmensabteilungen unautorisierte Cloud-Lösungen *mit entsprechenden eingehandelten Risiken* zu realisieren (IT-Schattenwirtschaft).

Sehr gerne stehe ich Ihren Cloud-Vorhaben kompetent, engagiert und nachhaltig zur Verfügung.

EIGENE DATENSPEICHERUNG ODER EXTERNES RECHENZENTRUM: WELCHE LÖSUNG BIETET DIE GRÖSSTE DATENSICHERHEIT?

Das kommt auf die genaue Ausprägung der Absicherung Ihrer eigenen Datenhaltung versus die genaue Ausprägung der durchgeführten und wirksamen Sicherheitsmaßnahmen des jeweiligen (natürlich mit mehr Sicherheitsbudget operierenden) externen Rechenzentrums an.

Denken Sie daran bei Abwicklung Ihrer Geschäftsprozesse unter erforderlicher Vernetzung mit dem externen Rechenzentrum müssen Sie den Risiken des Datenaustauschs durch eine sicherzustellende Transport-Absicherung begegnen (Vertraulichkeit sicherstellen! - Sie sollten bei einer Internetverbindungslösung mindestens ein https-Protokoll fahren unter Prüfung, dass dabei auch tatsächlich sichere kryptographische Verfahren angewendet werden). Ebenso müssen Sie dem Risiko einer Verfälschung (Datenintegrität sicherstellen!) durch Vorkehrungen Rechnung tragen. Vor dem Risiko untragbarer Reaktions- und Latenzzeiten, eines Ausfalls oder einer verminderten Leistung seitens des Dienstleisters - Ihr "Provider" - müssen Sie sich mit klar geregelten Verfahren bzw. Leistungsmerkmalen in Ihrem Dienstleistungsvertrag gegenüber Ihrem Provider schützen (Verfügbarkeit sicherstellen!).

Ferner sollten Sie auch die Möglichkeit eines sauber geregelten Wieder-Insourcings (also der Wiedereinverleibung ins Unternehmen) bei der Vertragsgestaltung mit Ihrem Provider absichern. Denn je mehr Freiheiten und Dienstleistungsumfang Sie Ihrem Provider überlassen, umso mehr steigt auch Ihre Abhängigkeit und die Versuchung Ihres Providers den Preis nach und nach anzuziehen.

WARUM IST DIE AKZEPTANZ VON GEBRAUCHTER SOFTWARE SEHR NIEDRIG?

Nun gebrauchte Software zeichnet sich durch ein gewisses Alter aus. Die Bedienungsoberfläche und deren Mechanismen können veraltet sein. Wenn diese gebrauchte Software Ihre Bedürfnisse doch voll abgedeckt, warum nicht?

Aber die Risiken dabei müssen Sie im Auge behalten, um mal einige zu benennen:

- Wie können Sie prüfen, dass die Software keinen Schadcode enthält?
- Befindet sich die gebrauchte Software zumindest für Sicherheitsaktualisierungen noch im Update-Zyklus des Herstellers? Wie lange noch?
- Kann die Übereignung dieser Software an Sie ohne Friktionen mit dem Hersteller herbeigeführt werden?
- Wie stellen Sie eine Ablösung der alten Software sicher, wenn die Sicherheitsaktualisierungen dann tatsächlich auslaufen?

Zum Autor

Dipl.-Ing. Frank W. Holliday, zertifiziert als *TeleTrusT Information Security Professional* (T.I.S.P.), *CISSP* und *ISO/IEC 27001 Lead Auditor*, ist seit über 15 Jahren im Bereich Informationssicherheit und Datenschutz tätig und blickt auf eine über 35 Jahre umfassende Erfahrung in vielfältigen Verwendungen im Bereich IT, Informationssicherheit und Datenschutz zurück. Er beschäftigt sich insbesondere mit der Aufsetzung nachhaltig sicherer Informationstechnologie-Systeme. Er ist Mitglied der *Gesellschaft für Informatik e.V.* (GI) und arbeitet in der Fachgruppe *Management von Informationssicherheit (SECMGT)* des GI-Fachbereichs *Sicherheit – Schutz und Zuverlässigkeit*, sowie bei der Arbeitsgruppe *ISM* des *TeleTrusT e.V.* mit.

Kontaktdaten

Frank W. Holliday
Wilhelmstr. 1A, D-64853 Otzberg
E-Mail: f.w.holliday@holliday-consulting.de
Internet: https://www.holliday-consulting.com
Mobiltelefon: 0172 956 037 0