Homeoffice Arbeitsplätze

Printout von blog.jakobs.systems

Tomas Jakobs

03 Mai 2021

Inhaltsverzeichnis

Blog-Serie in drei Teilen

Wie kann ein Homeoffice in einem Unternehmen sicher integriert werden? Und das bitte auch günstig, transparent und nachhaltig! Mit dieser Frage haben sich dank Corona-Lockdown einige beschäftigen dürfen.

Als externer Dienstleister stehe ich oft genug am Spielfeldrand und blicke hinein in die große Arena der Digitalisierung wo leider auch viel Schwarmdummheit[1] und Flachsinn[2] unterwegs sind und technische Schulden[3] sowie Komplexität anhäufen.

Mit diesem Bild vor Augen beginne ich eine neue Blogserie und beschreibe, wie aus meiner Sicht der perfekte Homeoffice-Arbeitsplatz für kleine und mittelständische Unternehmen aussehen kann. Es gilt wie immer: Keine Lösung passt universal auf jeden Use-Case. Your milage may vary und selbstverständlich der Hinweis: Ich bin für genau diese Dinge käuflich.

Beginnen möchte ich mit den Basics was in der Informationssicherheit als Standard definiert ist. Orientierung gibt die VdS 10000 Informationssicherheitsmanagementsystem für kleine und mittlere Unternehmen[4]. Mit einem Exkurs in die Welt des Hackings zeige ich, warum es keine gute Idee ist, einen Windows Arbeitsplatz aus der internen Domäne in fremde Netze zu verpflanzen und mit VPN einzubinden. Zum Abschluss des ersten Teils zeige ich das Konzept eines mobilen Standortes.

Im zweite Teil arbeite ich mich thematisch an Terminalservern ab. Primär möchte ich zeigen, wie kostengünstig und auch kurzfristig alle Arbeitsplätze eines Unternehmens zu Homeoffice-Arbeitsplätzen werden können. Mit Mehr-Faktor-Authentifizierung, TLS-Verschlüsselung, zentralem Management und vor allem ohne irgendwelche Client-Software-Blackbox-Installationen auf den Endgeräten. Und weil der Einstieg in den Ausstieg von proprietärer Software über Terminalserver geht, zeige ich auch wie unkompliziert, kostengünstig und schnell ein Debian Linux-Terminalserver mit einer vollständigen Büroumgebung hochgezogen ist.

Im dritten und letzten Teil messen wir die Risiken und Folgen einer Maßnahme. Das klingt jetzt nicht sonderlich spannend und in Anbetracht der Themenfülle der vorhergehenden Punkte hört es sich auch nach wenig an. Ist es aber nicht. Ein Top-Management braucht leicht

---

[1] https://www.campus.de/e-books/wirtschaft-gesellschaft/wirtschaft/schwarmdumm-9794.html

[2] https://www.campus.de/buecher-campus-verlag/wirtschaft-gesellschaft/wirtschaft/flachsinn-10854.html

[3] https://de.wikipedia.org/wiki/Technische_Schulden

[4] https://de.wikipedia.org/wiki/VdS_10000

verdauliche Fakten und ein Netzwerkadmin klare Vorgaben und Regeln.

Wie immer, konstruktive Kritik, Anmerkungen und Diskussion erwünscht. Alles bitte im Kuketz-Forum.

Was sagt das Informationssicherheitsmanagement?

Grundsätzlich MÜSSEN bei Homeoffice-Arbeitsplätzen Informationssicherheits-Richtlinien vom Unternehmen erarbeitet werden und zwar ausgehend und mit dem Commitment des Top-Managements[5]. Dieses muss die Richtlinien nicht nur freigeben sondern auch Sorge dafür tragen, dass jeder Mitarbeiter sie auch versteht. Das setzt eine Angemessenheit voraus, die zur jeweiligen Arbeitssituation passt. Eine Anweisung „Du musst Dateien AES 256[6] verschlüsseln“ wird niemand verstehen oder ausführen können.

Ohne Schulung und Sensibilisierung sollte niemand in ein Homeoffice geschickt und sich allein überlassen werden. Natürich wird niemand von sich aus zugeben, Defizite im Umgang mit seinem täglichen Handwerkszeug zu haben aber das ist ein anderes Thema.

Klare Erfolgs- oder Abbruchkriterien und zur Not auch Sanktionsmöglichkeit sollten auf jeden Fall parat liegen. Nicht jeder ist in der Lage aus dem Homeoffice zu arbeiten. Das ist ein Fakt und nichts Schlimmes. Es wird nur dann zum Problem, wenn es unberücksichtigt bleibt.

Homeoffice Arbeitsplätze werden als mobile IT-Systeme verstanden, die gegenüber Gefährdungen wie Diebstahl, unautorisiertem Zugriff oder Netzwerkübergänge (Heimnetz, Mobilfunknetz) besondere Schutzmaßnahmen[7] über einen Basisschutz[8] hinaus notwendig machen. Ein einfaches Ausreißen eines Rechners aus dem internen Netzwerk und ein VPN erfüllen diese Vorgaben gerade nicht. Es müssen zusätzlich Regelungen für Datensicherungen[9] und Mehr-Faktor-Authentifizierungen[10] für Fernzugänge gefunden werden.

Erfolgt eine Einwahl via VPN, also eine Kopplung mit dem Netzwerk der Organisation, muss

[5] VdS 10000, 6.1 sowie 6.4

[6] https://de.wikipedia.org/wiki/Advanced_Encryption_Standard

[7] VdS 10000, 10.4 „Zusätzliche Maßnahmen für mobile IT-Systeme“

[8] VdS 10000, 10.3 „Basisschutz von IT Systemen“

[9] VdS 10000, 16.5.4 „Datensicherung mobiler IT-Systeme“

[10] VdS 10000, 11.4.3 „Fernzugang“

diese netzwerktechnisch zusätzlich abgesichert werden[11]. Explizit werden IDS/IPS Systeme genannt und empfohlen. Und in einem segmentierten Firmennetzwerk reden wir selten nur von einem System, es sollten mehrere sein, mindestens eines in jeder logischen Entität oder Standort. Entgegen den allgemeinen Empfehlungen so mancher Fachhändler, die einem Kunden mit teuren Abo-Modellen von Fortinet, Sophos & Co auf Extra-Hardware mitten hinein in die digitale Abhängigkeit locken, rede ich von Open-Source IDS/IPS Systemen, die weder teuer noch aufwändig und vor allem auf Standard-Hardware zu betreiben sind.

Last but not least: Bei mobilen IT Systemen und bei zunehmenden Video- und Screensharing Tätigkeiten stellt sich mehr als zuvor die Frage: Was tun bei Verlust des Gerätes oder der Zugangsdaten? Wer informiert wen, wo müssen zeitnah Konten gesperrt werden?[12]. Was ich häufiger sehe: Copy & Paste während gemeinsamen Screensharing- oder Fernsteuerungen. Ob bekannt ist, dass Inhalte aus der Zwischenablage je nach verwendeter Software mit den Teilnehmern geteilt werden? Mir hat ein nettes kleines Tool, das jede Sekunde den Inhalt aus der Zwischenablage in eine Textdatei pollt schon manche hilfreiche Dienste geleistet.

Respekt bei allen, die bereits über entsprechende IS-Richtlinien vor Corona verfügten und diese auch ohne Diskussionen umsetzen konnten und vor allem resistent gegenüber dem Argument: „Außerordentliche Zeiten erfordern außerordentliche Maßnahmen“ geblieben sind. Wer jedoch kein funktionierendes Informationssicherheitsmanagement hat und die Zeit des Lockdowns auch nicht als Initialzündung zum Aufbau eines solchen genutzt hat, der wird mit hoher Wahrscheinlichkeit zu jenen gehören, die Ihre Digitalisierung gerade mit Ankündigung und richtig viel Anlauf am verkacken sind. Die Preisfrage lautet nicht „ob“ sondern „wann“ es knallen wird.

Als Sportpilot ziehe ich gerne den Vergleich zur Fliegerei. Auch da müssen Risiken und Gefahren abgewogen und im Umgang mit komplexer Technologie beherrscht werden. Wer einen Flug vorher nicht plant, Wetter und NOTAMs nicht einholt und auch sonst nie den Umgang mit Checklisten erlernt und als Konzept und Ausweg aus einem „Trajectory of accident opportunity“[13] begriffen hat, der wird möglicherweise viele Jahre lang um den heimischen Platz herum fliegen können. In der ersten brenzligen Situation außerhalb seiner Komfortzone jedoch scheitern.

---

[11] VdS 10000, 11.4.4 „Netzwerkkopplung“

[12] VdS 10000, 10.4.3 „Verlust“

[13] James Reason, „Human Error“, 20th printing 2009, Cambridge University Press, Seite 208

Ein böses Sprichwort in der Fliegerei besagt: „Die Luft reinigt sich von selbst“. Mir ist leider kein vergleichbares Sprichwort aus der Informationssicherheit bekannt.

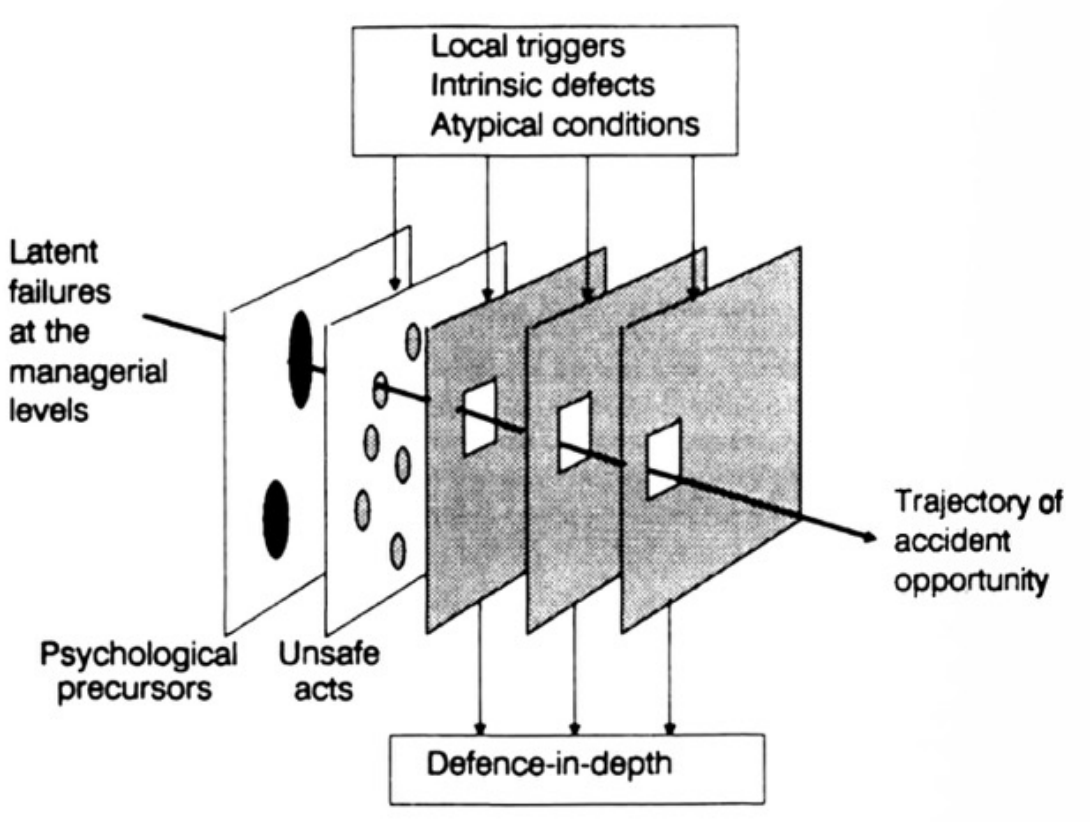

Abbildung 1: Grafik Error-Trajectory

Interner Windows-Rechner mit externer VPN-Einwahl

Der übliche Homeoffice-Arbeitsplatz besteht aus einem Windows-Notebook, vom firmeninternen Active-Directory (AD) verwaltet und mit einem VPN-Zugang zur Einwahl über das heimische WLAN ausgestattet. Diese Konstellation wirft folgende Probleme auf:

- Private Netzwerke verfügen über kein angemessenes Schutzniveau. Die Bandbreite reicht von veralteten oder falsch konfigurierten Routern über bestehende Malware auf anderen Rechnern bis hin zu unbekannten Netzwerk Konfigurationsfehlern.

- So betriebene Rechner sind „dual homed“[14], sprich mit mehreren Interfaces in unterschiedlichen Netzen verbunden, meist mit dem privaten WLAN und dem Firmennetzwerk.
- Die Sicherheit des Gesamtnetzes ist abhängig von der Sicherheit des schwächsten Gliedes. Jedes dual homed Gerät wird zum bevorzugten Angriffsziel, da es in der Regel leichter zugänglich und schlechter geschützt ist als die extra gehärteten und kontrollierten Netzwerkübergangspunkte.
- Zuletzt ein häufig vergessener rechtlicher Aspekt bei Verwendung von Microsoft Windows, die nicht den Programmversionen „Enterprise“ oder „Professional“ entsprechen: Wer eine Windows Home gewerblich einsetzt, der begeht einen Lizenzverstoß und somit einen Rechtsbruch.

Exkurs: WLAN-Hacking

An dieser Stelle ein kurzer Ausflug in die Welt des Pentestings und WLAN-Hackings. Neben dem Know-How reicht prinzipiell nur ein wenig Bastelgeschick zum Erstellen eines WLAN-Sniffers. Ich bin faul und nutze ein fertiges Pineapple[15] und habe den Vorteil damit viele Funktionen automatisieren zu können und schöne Übersichten zu erhalten.

[14] https://de.wikipedia.org/wiki/Dual_homed_host

[15] https://shop.hak5.org/products/wifi-pineapple

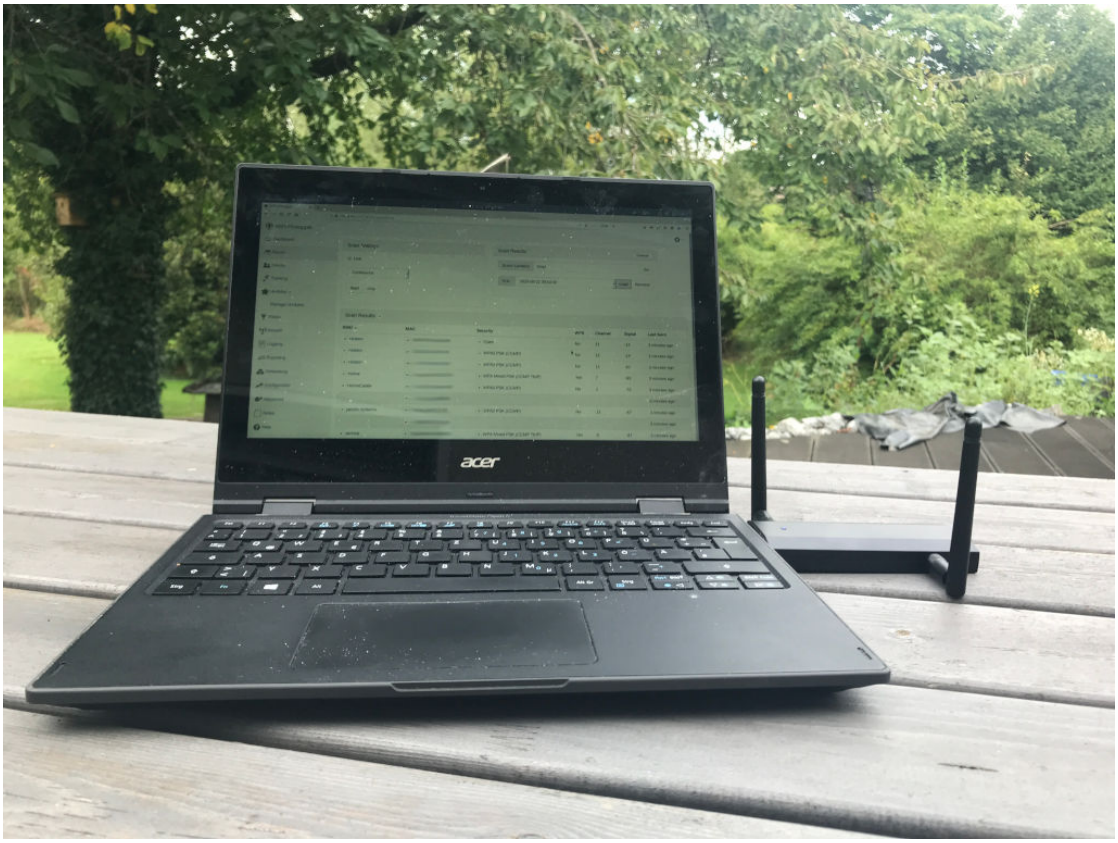

Abbildung 2: Pineapple im Einsatz

DIe Vorgehensweise ist immer gleich:

- Ermitteln des Zielgerätes aus der Menge funkender Geräte
- Aufzeichnen und Untersuchen aller von diesem Gerät gesuchten WLAN/MAC-Addressen
- Spoofen eines dem Gerät bekannten WLAN mit einem RogueAP[16]
- Deauth-Angriff[17] zum Trennen und Neuverbinden mit dem eigenen RogueAP

An dieser Stelle ein Disclaimer: Deauth-Angriffe stellen strafrechtlich einen Hackerangriff dar und sind darüber hinaus von der Bundesnetzagentur untersagt[18]. Diese dürfen nur im eigenen

[16] https://en.wikipedia.org/wiki/Rogue_access_point

[17] https://www.elektronik-kompendium.de/sites/net/2109171.htm

[18] https://www.golem.de/news/bundesnetzagentur-nutzung-von-deauthern-ist-nicht-zulaessig-2001-145911.html

Netz und Gerät und unter Laborbedingungen mit schwachen Sendeleistungen ausgeführt werden. Eleganter ist es, einen RogueAP an unerwarteten Orten mit der SSID/MAC des Heimnetzes aufzustellen und einfach zu warten bis sich ein Notebook automatisch verbindet.

Lustigerweise ist ein solcher idealer Ort das Büro in der Firma und zwar genau dann, wenn dort ein Notebook mit Kabel in das Firmennetzwerk eingestöpselt wird, das WLAN dabei aber eingeschaltet bleibt. Da rächt es sich, dass Windows keine Netzwerkprofile oder up/down Regeln kennt. Mit dem bekannten Heimnetz wird sich ohne Nachfrage verbunden.

Einen so positionierten RogueAP (ironischerweise in einem Pistolen-Waffenkoffer) kann ich tagelang betreiben. Sobald der Zielrechner „am Haken“ hängt, erhalte ich als frischgebackener Man-in-the-Middle[19] eine kurze Email-Benachrichtigung. Das ist der aufwändigere Part.

Abbildung 3: RogueAP im Koffer

[19] https://en.wikipedia.org/wiki/Man-in-the-middle_attack

Über den Rechner in das Firmennetzwerk

Zur Übernahme eines Rechners werden lokale Administrationsrechte benötigt. Leider werden diese immer noch viel zu leichtfertig vergeben. Der Grund muß nicht immer alte Software sein. Moderne, bunte und farbige Gaming-Mäuse oder Tastaturen[20] können aus der Ferne bereits untrügliches Erkennungszeichen dafür sein, dass jemand möglicherweise mit lokalen Adminrechten arbeitet. In der Regel sind es dann auch meist Power-User oder solche, die als besonders fortgeschritten, trendy oder erfahren gelten.

Nicht wirklich komplizierter wird es, wenn es lokale Adminrechte noch zu erlangen gilt. Dazu bedarf es meist einer Schwachstelle zur Priviledge Escalation[21]. Fahrlässige Administratoren sind ebenfalls willkommen wenn Passwörter im Klartext an verschiedenen Orten im System hinterlegt sind. Die Möglichkeiten sind auf verwalteten Domänenrechnern vielfältiger da ein privates Gerät in der Regel keine Dienstkonten, Anmelde- oder Updateskripte, Remote-Datensicherungen, Zeiterfassungen, Monitoring oder Inventarisierung hat.

Es gibt genügend Youtube-Videos[22] und Internet-Anleitungen[23], die eine Übernahme eines Windows-Rechners viel besser erklären können. Nicht jedes Tool passt auf Anhieb auf das jeweilige Ziel.

Als Fakt bleibt festzuhalten: Einmal auf einem Windows-Arbeitsplatz, das zugleich Domänenmitglied eines Firmennetzes ist, und das Spiel ist gelaufen. Vergleichbar mit einem 5:1 in der 85. Spielminute in einem Fußball-Länderspiel: Debug-Privilegien einholen, mimikatz[24] ausführen und Kennwörter im Klartext auslesen.

Ein schwacher Trost: Damit ist das Spiel noch nicht ganz vorbei. Bonusmeilen gibt es erst mit dem Kerberos TGT User[25] und dem „golden Ticket“. Das ist der Todesstoß einer jeder AD Infrastruktur. Ab da hilft nur Neuinstallation aller Server und Arbeitsplätze.

Leider genau das, was Betroffene immer wieder und wieder und wieder machen in der Hoff-

[20] https://insider.razer.com/index.php?threads/every-time-i-start-cortex-it-asks-for-admin-permissions.54669/

[21] https://de.wikipedia.org/wiki/Rechteausweitung

[22] https://www.youtube.com/watch?v=saF9epFwzPE

[23] https://adsecurity.org/?p=4367

[24] https://github.com/gentilkiwi/mimikatz

[25] https://www.christophertruncer.com/golden-ticket-generation/

nung, dass sich was ändert. Vaas Montenegro lässt grüßen[26]. Weiterer Fun-Fact: Die Tools mimikatz und kekeo sind eigentlich nur „side-projects“ von Benjamin Delphy, dem Entwickler dahinter, der ursprünglich nur etwas C und Microsoft Windows kennen lernen wollte[27].

Zurück zu unserem Homeoffice Rechner. Office-Dokumente in Email-Anlagen vertraut niemand mehr. Dem vermeintlich sicheren Heimnetzwerk jedoch umso mehr. Bereitwillig werden SMB Netzwerklaufwerke und Druckerfreigaben geteilt und Firmenadmins nehmen an, eine vertrauenswürdige Umgebung für Ihr VPN vorzufinden. Eine Zeile netsh reicht für eine Netzwerkbrücke[28] aus.

Sicherungsmaßnahmen

Für mich persönlich ist Windows als Betriebssystem strukturell kaputt und nur isoliert ohne direkte Internetverbindung sicher zu betreiben. Damit werden auch etwaige datenschutzrechtlichen Fragen abschließend beantwortet. Diese Radikalität ist natürlich selten praktikabel und die Situation ist nicht ganz so hoffnungslos, wie sie jetzt erscheinen mag.

Ein Application-Whitelisting zum Beispiel ist seit Windows XP Bestandteil in jedem Windows, unabhängig davon ob Domänenmitglied oder nicht. In einem AD verwaltet und ausgerollt nennt es sich Software-Restriction-Policy[29]. Das würde zum Beispiel ein Ausführen von mimikatz und anderen Tools unterbinden.

Eine weitere Möglichkeit ist es auf WLAN komplett zu verzichten und ein Homeoffice nur über sicher verkabelte und kontrollierte Endpunkte einzurichten die erst Ihrerseits mit einem Fremdnetz verbunden sind.

Konzept des mobilen Standortes

Auf die Idee brachte mich das Szenario eines Kunden aus der Baubranche. Für größere Baustellen wurde Vor-Ort ein Netzwerk mit drei Segmenten benötigt. Neben den eigenen Bauleitern

[26] https://www.youtube.com/watch?v=d796zw4Vzqw

[27] https://www.wired.com/story/how-mimikatz-became-go-to-hacker-tool/

[28] https://docs.microsoft.com/en-us/windows-server/networking/technologies/netsh/netsh

[29] https://docs.microsoft.com/de-de/windows/security/threat-protection/windows-defender-application-control/applocker/using-software-restriction-policies-and-applocker-policies

des Kunden sollten auch fremde Projektbeteiligte Zugriff in das Internet erhalten, natürlich drahtlos. Und wie selbstverständlich sollte neben POE Webcams auch gemeinsame Drucker/Scanner mitsamt SMB-Netzwerkfreigabe für Scanordner hinzukommen. Alles Potential für heftige Security-Alpträume in einer Umgebung, die bestenfalls als „rau“ zu bezeichnen ist. Begleitender Faktor zur Steigerung der allgemeinen Ungemütlichkeit war noch die Wirkung von Metall-Baucontainern und allerlei Heavymetal Baugerät in der Umgebung auf Mobilfunk- und WLAN-Signale[30]. Eine robuste, flexible und zugleich in der Handhabung simple Lösung („das rote Kabel hier, das grüne Kabel dorthin“) musste gefunden werden, die Baustellen-Box:

[30] https://de.wikipedia.org/wiki/Faradayscher_K%C3%A4fig

Abbildung 4: Baustellen-Box

Ein vollständiges Netzwerk bestehend aus LTE-Fritzbox, 8-Port POE Switch, einer ipfire.org[31] Firewall und einigen weiteren Extras. Sicher aufbewahrt in einem abschliessbaren 10", 6 HE Netzwerkschrank aus Metall. Die Gegenstelle im Unternehmen besteht ebenfalls aus einer ipfire und ermöglicht mit Firewall- und Routingregeln den feingranularen Zugriff auf ausgewählte

[31] https://www.ipfire.org/

Ressourcen. Auf beiden Seiten voneinander unabhängig laufen zwei IDS/IPS[32] mit SNORT und melden bzw. sperren verdächtige Pings, Netzwerk- oder Portscans.

Mein eigenes Homeoffice

Eine solche Box steht auch in meinem Homeoffice. Ein schönes Detail: Der 10" Netzwerkschrank des sauerländischen Herstellers passt wie angegossen in ein IKEA KALLAX/EXPEDIT Regal.

Abbildung 5: Homeoffice-Box

Abweichend von der zuvor vorgestellten Baustellen-Box nutze ich andere Innereien in Gestalt einer Managed-Switch und einer höherwertigen Firewall mit 4x Gigabit Interfaces. Das Prinzip

[32] https://wiki.ipfire.org/configuration/firewall/ips

bleibt aber gleich: Nur das sichere, fest verkabelte grüne Segment ist per VPN mit meinem Büro verbunden. Die Radios der verbundenen Geräte bleiben ausgeschaltet.

Mit Switch, Steckdosenleiste und Einlegeboden liegt so ein kleines Schränkchen preislich um die 150-200,- EUR. Ein Barebone für die ipfire.org gibt es ebenfalls in dieser Preisklasse. Hinzu kommen Zeit für Planung, Montage und Einrichtung. Alles zusammen ein Bruchteil der Kosten und Schäden, die im worst-case drohen.

Der größte Vorteil: Solange ausschließlich Standard-Hardware und freie Open-Source Software verwendet werden, bleibt man unabhängig von der Preis- und Produktpolitik großer Tech-Konzerne mit Ihren eigenen Vorstellungen von Lebenszyklen, IT-Sicherheit und Datenschutz.

Das verstehe ich unter einer nachhaltigen, flexiblen und langfristigen Digitalisierung.

Teil II - Ein Blick zurück

Der zweite Teil der Homeffice-Serie dreht sich um Terminalserver. Dabei ist das Konzept alt, sehr alt. Wir kommen um einen kurzen Ausflug in die Vergangenheit nicht herum:

Es geht zurück zu den Anfängen der Computergeschichte Ende in die 40er und 50er Jahre des letzten Jahrhunderts. Rechnerzeit auf den damaligen VN-Großrechnern[33] war als Ressource knapp, teuer und oft geheim. Ohne zu sehr ins Detail gehen zu wollen, empfehle ich das Buch von Kai Schlieter „Die Herrschaftsformel“[34], der die Entwicklungsstränge von Computertechnologie, Wehrtechnik, Kybernetik und Public-Relations aufzeigt.

Für uns wichtig ist die Erkenntnis der 50er Jahre, dass nur Multi-User und Multitasking-Systeme wirtschaftlich sinnvoll zu betreiben waren. Mehrere Programme wurden auf einem zentralen Großrechner in kurzen Zeitfenstern nacheinander ausgeführt damit mehrere Anwender mit Ihren Anwendungen an jeweils Ihren Ein- und Ausgabegeräten, einem Terminal, arbeiten konnten. Dieses „time-sharing“ Prinzip[35] bildet die Grundlage eines jeden modernen Betriebssystems.

Doch mit dem Mikrochip ab 1971[36], spätestens mit der explosionsartigen Verbreitung der Home- und Personal-Computer in den 70er und Anfang der 80er Jahre verlagerte sich das Paradigma auf die Single-User-Mode[37] Computer. Betriebssysteme wie CP/M ab 1974[38] oder dessen dreist kopierter Klon MSDOS ab 1981[39] sind die bekannteren Vertreter dieser Entwicklung. Mein erster PC aus dem Jahr 1988, ein Schneider EURO-PC mit MSDOS 3.3 entspringt aus genau dieser Zeit.

---

[33] https://en.wikipedia.org/wiki/Von_Neumann_architecture

[34] https://www.westendverlag.de/buch/die-herrschaftsformel-2/

[35] https://en.wikipedia.org/wiki/Time-sharing_system_evolution

[36] https://www.computerhistory.org/siliconengine/microprocessor-integrates-cpu-function-onto-a-single-chip/

[37] https://en.wikipedia.org/wiki/Single-user_mode

[38] https://en.wikipedia.org/wiki/CP/M

[39] https://en.wikipedia.org/wiki/MS-DOS

Abbildung 6: Mein erster PC, ein Schneider EURO-PC mit MSDOS 3.3

Es waren diese günstigen Single-User-Mode Geräte, die zusammen mit grafischen Oberflächen Einzug in Mainstream und Unternehmen fanden. Und wie in den 50er Jahren wusste jeder: Nur mit geteilten Multi-Usern und vor allem Multitasking Systemen funktioniert auch ein ernsthaftes und wirtschaftliches Arbeiten. Es ist ein Fakt, dass ein Rechner die meiste Zeit seines Daseins im idle[40] verbringt.

Aus diesem Grund begann ab 1984 in der Unix-Welt die Entwicklung des X Window-Systems[41], einer Abstraktionsschicht zum Übermitteln von grafischen Bildschirminhalten und Steuerbefehlen an lokale und entfernte Terminals. Anders als bei den Großrechnern, kann dieses auch über ein Netzwerk erfolgen. Ein kleines Start-Up mit dem Namen Citrus kopierte und

[40] https://de.wikipedia.org/wiki/Leerlaufprozess

[41] https://en.wikipedia.org/wiki/X_Window_System

optimierte ab 1989 dieses Prinzip auf MSDOS basierte Systeme. Die Independent Computing Architecture, das ICA-Protokoll[42] war geboren. Kurze Zeit später erfolgte die Umbenennung des Unternehmens in den heutigen Markennamen Citrix[43]. Microsoft lizenzierte diese Technologie rasch, integrierte es als Terminal Services[44] in seiner Windows NT Produktfamilie und nannte es seinerseits Remote-Desktop-Protokoll[45].

Eine Frage der Perspektive

Citrix und Microsoft teilen sich den Markt der Windows-basierten Terminalserver auf. Lange Zeit galt Citrix als das schlankere und performantere Protokoll und profitierte von seiner Stellung als Technologievorreiter. Der „seamless" Fenstermodus und die nahtlose Integration mit lokalen Apps war ein Killer-Feature. Spätestens mit der 2016er Servergeneration hat Microsoft aber gleichgezogen.

Citrix hat auch früher als Microsoft einen Technologievorsprung im Bereich der Virtualisierung geschaffen. Auch hier hat Microsoft meiner Meinung nach gleichgezogen. Doch ist die Frage der Virtualisierung ein anderes Thema, das sich hier nicht stellt.

Ich vermag nicht zu sagen, welche Seite besser ist. Es ist eine Frage der Perspektive und woher jemand mit seinem Netzwerk kommt. Solche A/B Fragen werden ohnehin oft evidenzfrei wie Glaubensfragen entschieden und gehen selten auf spezifische Ausgangsprobleme ein. So gibt es neben Microsoft und Citrix auch Thinstuff[46]. Meine persönliche Präferenz, wenn es „mal eben" gilt ältere Fachanwendungen auf teilweise noch älteren Serversystemen netzseitig zu segmentieren und als Terminalserver erreichbar zu machen.

Die bessere Fragestellung sollte sein: Was genau soll ein Terminalserver bringen? Immer wenn ich vollständige Desktops in Terminals mit allen Anwendungen, Webbrowser und Email-Anwendung sehe, frage ich mich, welche Gedankengänge hinsichtlich Informationssicherheit wohl dahinter stecken. Und dann werden diese Systeme in aller Regel für jeden aus dem Inter-

[42] https://en.wikipedia.org/wiki/Independent_Computing_Architecture

[43] https://en.wikipedia.org/wiki/Citrix_Systems#Early_history

[44] https://news.microsoft.com/1998/06/16/microsoft-releases-windows-nt-server-4-0-terminal-server-edition/

[45] https://en.wikipedia.org/wiki/Remote_Desktop_Protocol

[46] https://www.thinstuff.com/products/xpvs-server/

net erreichbar gemacht, ohne Portknocking[47], GeoIP-Blocking[48] oder IDS/IPS Systemen mit Snort-Regeln[49] davor.

Citrix hatte unlängst mit einer ungepatchten Sicherheitslücke zu kämpfen gehabt, die auf einen Schlag alle aus dem Internet erreichbaren Systeme verwundbar machte. Sogar das BSI musste warnen[50], da über 5000 Unternehmen alleine in Deutschland davon betroffen waren. Eine Recherche mit diesem netten Skript[51] offenbarte mir ein halbes Jahr später im Juli 2020 noch dutzende, ungepatchte Systeme in Shodan[52].

Die Sicherheitslage bei Microsoft ist nicht besser. Es war und ist weiterhin das bevorzugte Einfallstor für Hacker[53]. Bei Entdeckung der „Bluekeep“ Schwachstelle letztes Jahr, einem fundamentalen Designfehler bei der Implementierung, sah sich Microsoft sogar genötigt die längst nicht mehr unterstützten Windows-Versionen XP und 2003 Server zu patchen[54]. Doch auch ohne Bluekeep gehörten FBI-Warnungen beinahe zum wiederkehrenden Ritual[55].

Sicherheitsproblematik

Es bleibt festzuhalten:

- Ohne zusätzliche Schutzmechanismen stellen aus dem Internet zugängliche Terminalserver ein erhebliches Risiko dar.
- Sowohl Citrix als auch Microsoft Terminalserver sind proprietäre Blackboxen. Evidenzbasierte Aussagen zur Sicherheit können nicht getroffen werden. Beide operieren nach

[47] https://en.wikipedia.org/wiki/Portknocking

[48] https://en.wikipedia.org/wiki/Geo-blocking

[49] https://en.wikipedia.org/wiki/Snort_(software)

[50] https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/Citrix_Schwachstelle_160120.html

[51] https://github.com/aqhmal/CVE-2019-19781

[52] https://shodan.io

[53] https://www.heise.de/hintergrund/Remote-Desktop-RDP-Liebstes-Kind-der-Cybercrime-Szene-1-4-4700048.html

[54] https://en.wikipedia.org/wiki/BlueKeep

[55] https://www.ic3.gov/media/2018/180927.aspx

dem Prinzip „Security by obscurity“[56].

Lösungswege

Wenn Technologien oder Systeme inhärente Sicherheitsrisiken haben stellt sich die Frage, welche risikomindernde Maßnahmen helfen, diese auf ein akzeptabeles Risiko zu bringen. Diese Liste stellt nur einen Ausschnitt an Möglichkeiten dar:

- Mehr-Faktor-Authentifizierungen z.B. TOTP
- Managed SSO[57] mit Einbruchserkennungen und Heuristiken
- Isolierung durch z.B. Verzicht auf eine AD-Integration
- Nutzung von IDS/IPS Systemen
- Beschränkung auf feste IPs z.B. mit VPNs
- Nutzung von kontrollierten Übergangspunkten (Gateways oder Proxies)
- Anwendungsinterne Sicherheitsfunktionen und Berechtigungskonzepte

Terminalserver - Ein Blick nach vorne

Ein entfernter Homeoffice-Arbeitsplatz kann über das Internet auf zwei Arten Verbindung mit einem Terminalserver aufnehmen:

- mit einer proprietärem Client-Software
- im handelsüblichen Webbrowser

Das eindeutig flexiblere Konzept ist eine Webbrowser-Integration mit gängigen Internettechnologien. So werden auch nicht von einer eigenen IT verwaltete Fremdsysteme in die Lage versetzt auf Ressourcen zugreifen zu können. Wer seine Infrastruktur in den letzten Jahren herstellerunabhängig auf das Bring-your-own-Device Prinzip[58] vorbereitet hat, verfügt heute über eine bessere Ausgangslage bei der Integration von Homeoffice-Arbeitsplätzen.

Als besonders traurig erachte ich den Umstand, dass im Jahr 2020 von vielen Unternehmen und Ihren Personalabteilungen es noch immer nicht verstanden wird, dass Fragen nach Homeoffice,

[56] https://en.wikipedia.org/wiki/Security_through_obscurity

[57] https://en.wikipedia.org/wiki/Single_sign-on

[58] https://de.wikipedia.org/wiki/Bring_your_own_device

Arbeitsumgebung und Betriebssystem harte Einstellungskriterien für qualifiziertes Personal darstellen. Schließlich kommt ja auch niemand auf die Idee Baggerfahrer einzustellen nur um diesen zum Ausheben einer Grube Schaufeln in die Hand zu drücken.

> Jeder sollte in genau der Systemumgebung arbeiten, mit der er am besten vertraut ist und seine Arbeit effektiv erledigen kann.

Für mich sind Terminalserver mit freien HTTPS-Gateways unverzichtbarer Bestandteil einer zukunftsfähigen Entwicklung.

Apache Guacamole

Zugegeben, Guacamole[59] ist ein Zungenbrecher. Als freie Software unter dem Dach der Apache Foundation stellt es aber ein um so besseres Gateway für RDP-, VNC- und SSH-Verbindungen über HTTPS zur Verfügung. Ich möchte hier zeigen, wie diese Lösung einem mittelständischen Unternehmen geholfen hat seine Mitarbeiter im Corona-Lockdown mit Ihren Desktop-Arbeitsplätzen im Büro zu verbinden.

Das ist durchaus wortwörtlich gemeint. Jeder Windows Desktop-Arbeitsplatz lässt sich mit einem Mausklick zum Terminalserver umfunktionieren. Ein so angemeldeter Benutzer arbeitet mit seiner gewohnten Arbeitsumgebung und Profileinstellungen. Guacamole dient als Gateway zwischen den Welten und wandelt das RDP-Signal auf Port 3389 aus dem internen Netz in ein TLS verschlüsseltes HTTPS auf Port 443 um.

Auf Anwenderseite im Homeoffice reicht ein handelsüblicher Webbrowser, zur Not auch auf dem heimischen Privat-PC. Es werden keine Anpassungen, Plugins oder zusätzliche Software-Client-Installation benötigt. Integriert als externe Anwendung in einer Nextcloud[60] findet ein Mitarbeiter alles in einer vertrauten und vor allem einheitlichen Oberfläche vor. Kalender, Emails und der Büro-Desktop in unterschiedlichen Browser-Tabs sind nicht nur technisch elegant sondern auch praktisch zum Hin- und Herswitchen.

[59] https://guacamole.apache.org/

[60] https://apps.nextcloud.com/apps/external

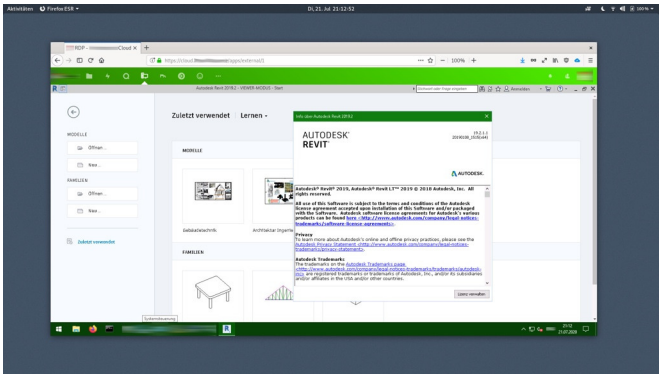

Abbildung 7: RDP Anwendung via Guacamole in Nextcloud Umgebung

Guacamole kann gegen OpenID, SAML oder wer es unbedingt möchte auch gegen ein LDAP authentifizieren. Aus Sicherheitsgründen empfehle ich letzteres ausdrücklich nicht. Ich habe bewusst die interne datenbankgestützte Authentifizierung gewählt, da ich gerade im Internet davon ausgehe, dass Anmeldedaten früher oder später verloren gehen.

Was Microsoft für sein RDP/RDS nur umständlich, undokumentiert und proprietär über Azure-Cloud[61] jenseits von Internetstandards kann, das bietet Guacamole von Haus an: Eine TOTP Mehr-Faktor-Authentifizierung. Standardkonform und sicher nach RFC 6238[62]. Wer bereits eine Nextcloud mit TOTP nutzt und auf einem Smartphone die benötigte FreeOTP[63] App sein eigen nennt, wird sich sofort zurecht finden. Erfreulich aus Adminsicht ist der fertige Jail in Fail2Ban[64] und auch die übersichtliche Reverse-Proxy Konfiguration[65].

Funktional mag das alles nichts anderes sein, was Microsoft nicht auch mit seinem HTML5 RD Web Paket anbietet. Wenn man von der kruden Mehr-Faktor-Authentifizerung jenseits aller Internetstandards absieht. Der fundamentale Fehler bei Microsoft ist jedoch die zwingende Integration auf einem im AD integrierten Server mit dem IIS. Aus meiner bescheidenen Sicht eine komplette Fehlkonzeption! Welchen Sicherheitsgewinn bringt ein derart vorgelagertes System wenn ein Angreifer bei Überwindung des Webservers mit einem Bein genau dort steht,

[61] https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

[62] https://tools.ietf.org/html/rfc6238

[63] https://freeotp.github.io/

[64] https://www.fail2ban.org/wiki/index.php/Main_Page

[65] https://guacamole.apache.org/doc/gug/proxying-guacamole.html

wo er auch hin will? Einem Tool wie mimikatz[66] ist es egal, wo es sein „Golden Ticket“ erzeugt solange es auf einem AD-Mitgliedsrechner ist.

Linux-Terminalserver

Ein Blog-Beitrag zu Terminalservern ohne gezeigt zu haben, wie einfach ein Terminalserver unter Debian eingerichtet ist? Für beliebig viele Anwender und frei von Lizenzkosten oder Abo-Fallen? Nein das geht nicht und deshalb zeige ich zum Abschluss eine Kurzanleitung. Als Anregung und Motivation zum selbst Ausprobieren. Ideal auch als Ersatzsystem oder als vorbereitende Maßnahme zur Migration. Als Hardware kann alles vom Raspi4 bis zum leistungsstarken Server genommen werden, je nachdem wie viele Benutzer gleichzeitig an diesem System arbeiten sollen. Es ist selbstredend, dass dieser Host netzwerktechnisch eine feste IP-Zuweisung oder zumindest über einen erreichbaren DNS-Namen verfügen sollte.

Eine Debian Standard-Server Grundinstallation ohne grafische Oberfläche und mit SSH-Server als einzige ausgewählte Installationsoption. Anschliessend installieren wir eine minimale GNOME Oberfläche mit nur den essentiellen Desktop-Tools und einem Firefox-Browser:

```
1 # apt install file-roller gthumb seahorse gnome-core
     gnome-dictionary
2 ffmpeg gnupg hunspell-de-de firefox-esr-l10n-de
     webext-ublock-origin
3 cifs-utils ssl-cert ca-certificates apt-transport-https -y
```

Installation von xrdp[67]. Das ist der die Software, die eine X11 Session in das RDP-Format umwandelt und dank Komprimierung und Caching dieses über ein Netzwerk besser übertragbar macht:

```
1 # apt install xrdp -y
```

Anpassung von Polkit, damit ein Benutzer mit jeweils seinem spezifischen Bildschirm nicht bei jeder Anmeldung nach Rootrechten gefragt wird. Dazu wird mit dem Texteditor der freien Wahl eine neue Regel-Datei erstellt:

[66] https://github.com/gentilkiwi/mimikatz

[67] https://xrdp.org/

```
cat <<EOF>> /etc/polkit-1/localauthority.conf.d/02-allow-colord.conf
polkit.addRule(function(action, subject) {
if ((action.id == “org.freedesktop.color-manager.create-device” ||
action.id == “org.freedesktop.color-manager.create-profile” ||
action.id == “org.freedesktop.color-manager.delete-device” ||
action.id == “org.freedesktop.color-manager.delete-profile” ||
action.id == “org.freedesktop.color-manager.modify-device” ||
action.id == “org.freedesktop.color-manager.modify-profile”)
&& subject.isInGroup(“{group}”))
{
return polkit.Result.YES;
}
});
EOF
```

Jetzt fehlen nur noch Benutzer mit Ihren unterschiedlichen Desktops zum Ausprobieren. Mit „adduser“ einfach mehrere erstellen, unterschiedliche Desktops z.B. mit anderen Hintergrundfarben erstellen und sich mit diesen von einem anderen Rechner aus über RDP auf Port 3389 verbinden.

Unter Windows kann hierfür mstsc.exe verwendet werden. Unter Linux nutze ich als bevorzugten Client Remmina[68], da es über eine übersichtliche Verbindungsliste und Speichermöglichkeit für mehrere Anmeldungen und Gegenstellen verfügt, ordentlich sortiert in Untergruppen.

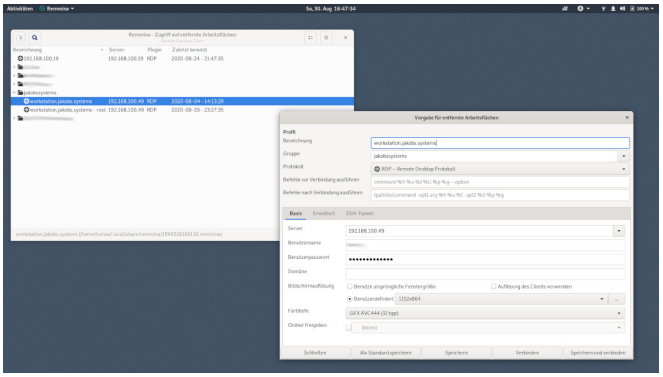

Abbildung 8: Ansicht von Remmina

[68] https://remmina.org/

Wie bei einem Windows-Terminalserver kann auch dieser Linux-Terminalserver hinter einem Guacamole-Gateway mit HTTPS betrieben werden, idealerweise zusätzlich abgesichert mit 2-Faktor-Authentifizierung. Wem dieses ein zu großes Risiko ist, der kann weiterhin den Zugriff von Außen über SSH oder VPN realisieren.

So bekommt frei von Lizenzfragen jeder Mitarbeiter eine Remote-Desktop Umgebung zum Arbeiten, unabhängig vom jeweiligen Rechner im Büro oder Homeoffice. Das alles als Impuls und mögliches Basislager für weitere Anpassungen und Integrationen.

Your milage may vary.

Teil III - Projektmanagment

Im dritten und letzten Teil meiner kleinen Blog-Serie geht es um Planung und Ausführung. Wir kommen dabei zwangsläufig in Berührung mit dem Projektmanagement und anderen mitschwingenden Rahmenbedingungen. Mein Versprechen aus dem ersten Teil löse ich ein und zeige zum Schluss eine Blaupause zur Risikoermittlung.

Ich wünsche viel Spaß beim Lesen! Es gilt wie immer der Disclaimer: Alles ohne Anspruch auf Vollständigkeit und Allgemeingültigkeit. Your milage may vary!

Digitalisierungsprojekte ohne IT-Abteilung

Wo anklopfen wenn es um ein Homeoffice geht? In der IT-Abteilung?

Bloß nicht! Was ist von jemanden zu erwarten, der sich nur im Hamsterrad des Alltags dreht, ohne Erfahrung jenseits des eigenen Horizonts? Mit solchen Sätzen mache ich mir keine Freunde. Ich formuliere neu:

Wo dürfen hochqualifizierte, teure Softwareentwickler, Admins oder Fachinformatiker an mindestens einem Arbeitstag in der Woche ohne Kosten- und Zeitdruck und ohne erkennbaren Bezug zum Unternehmen mit der Technik frei herumspielen und experimentieren?

Die Studie „Erfolgskriterien betrieblicher Digitalisierung“[69] des Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO hat bundesweit Unternehmen unterschiedlicher Branchen und Größen untersucht und festgestellt:

> Eine IT-Abteilung ist kein Haupttreiber der digitalen Transformation

Diese spielt bei Digitalisierungsprojekten erst eine Rolle, wenn es um operative Belange geht und das nur wenn…

> (…) Teckies Zeit, Raum und Budget gewährt bekommen.

> Das Ausprobieren an möglichst vielen und unterschiedlichen Stellen führt dazu, dass in der Organisation und unter den Mitarbeitenden ein Erfolgserlebnis entsteht, auch wenn einige Maßnahmen scheitern.

[69] https://www.bertelsmann-stiftung.de/fileadmin/files/user_upload/Erfolgskriterien_betrieblicher_Digitalisierung.pdf

> Es ist gut, wenn genügend Zeit ist, um sich spielerisch weiterzuentwickeln und keine wirtschaftlichen Gründe zum Handeln zwingen.

Commitment des Top-Managements

Ich muß nicht ausführen, wie diese Zitate im Management wirken. Freiräume für Freigeister führen zu Schnappatmungen in der Personalführung und Kopfschmerzen beim kaufmännischen Führungspersonal. Das mittlere Management bangt um seinen Einfluss. Zurecht wenn selbstorganisierende Projektteams gleichberechtigt mitreden und entscheiden. Ein Homeoffice sägt am Ast einer Präsenzkultur, wo so mancher Pfau sein innerbetriebliches Fürstentum bedroht sieht.

Alles Stereotypen und Heuristiken, die erschreckend mit dem übereinstimmen, was Sven Rimmelspacher als geschäftsführender Gesellschafter von Pickert & Partner in der Fraunhofer-Studie sagt:[70]

> Wir brauchen mehr Führung als früher, aber weniger Führer.

In Konsequenz spricht er von der Abschaffung aller mittleren Führungsebenen und traditioneller Abteilungs-Fürstentümer. Zugleich von der Stärkung cross-funktionaler und selbstorganisierter Projektteams sowie freien Einzelpersonen ohne Abteilungszugehörigkeiten. Disziplinarische Führung entfällt, Führungsaufgaben werden von agilen Teams übernommen. Wozu einen Personalleiter, wenn Projektteams den Job flexibler, zuverlässiger und schneller ausführen?

Das sind die strukturellen Schwachstellen und unausgesprochen Rahmenbedingungen, die im Hintergrund beim Thema Homeoffice mitschwingen. Vor dem Sprung in das Haifischbecken sollte das jedem klar sein.

Digitalisierungsprojekte scheitern meist entlang dieser Bruchlinien.

Ohne Rückendeckung des Top-Managements läuft’s nicht! Ein halbherziges Commitment, diffus, schwach oder schwankend und es ist Zeit zu gehen.

[70] Seite 38, Studie „Erfolgskriterien betrieblicher Digitalisierung“ in [ˆ1]

Projektteam Homeoffice

Kleine und schlagkräftige Teams, zusammengesetzt aus gleichberechtigten Personen und wechselnden Rollen und Repräsentanten nach Außen, den Product-Ownern[71] bilden die ideale Voraussetzung digitaler Keimzellen[72]. Dabei dürfen auch mehrere Teams parallel an einem Projekt arbeiten. Im Pentesting von IT-Infrastrukturen nicht unüblich. Ein rotes Team als Angreifer versucht ein blaues Team als Verteidiger zu überwinden. Die Erkenntnisse werden anschließend zusammen gebracht und gemeinsam ausgewertet.

Wichtig ist auch der Input und die Zusammenarbeit mit Externen, die im Bedarfsfall oder dauerhaft als Mentoren ein Projekt begleiten. Letztes Jahr wurde ich beispielsweise von einer Bauunternehmung bei Ihrer BIM-Digitalisierung[73] mit der Software Autodesk REVIT hinzugerufen. Es ging um den Aufbau und Inbetriebnahme einer Infrastruktur mit nahtloser Integration in die bestehende Umgebung. Systemhäuser oder Fachhändler können das nicht leisten. Und im Gegensatz zu eingekauften Lösungen „von der Stange“ oder aus der Cloud bleibt das Know-How und die Technik im Unternehmen.

Leider schaffen das der Fraunhofer-Studie zufolge nur etwas mehr als ein Drittel der Unternehmen[74]. Und das, obwohl Agilität[75] seit Jahren an Universitäten gelehrt wird.

Kommunikation und Dokumentenlenkung

Gehen wir vom Commitment der Geschäftsführung und dem Zustandekommen eines Projektteams aus. Wie geht’s weiter?

Ein Team muß untereinander und mit anderen kommunizieren, auf gemeinsame Projektdaten und Dokumente zugreifen und diese lenken können. Fehlen diese Grundlagen, müssen sie zuerst aufgebaut werden. Leider verstehen viele Ihre Rechner als Schreibmaschinenersatz und pflegen Verzeichnisstrukturen auf zentralen SMB-Netzwerklaufwerken wie Aktenschränke. Mir persönlich sind die typischen strukturierten QM/QS-Ordnerstrukturen ein Graus, wo nicht

[71] https://en.wikipedia.org/wiki/Scrum_(software_development)#Product_owner

[72] Seite 30ff, Studie „Erfolgskriterien betrieblicher Digitalisierung“ in [^1]

[73] https://de.wikipedia.org/wiki/Building_Information_Modeling

[74] Seite 31, Studie „Erfolgskriterien betrieblicher Digitalisierung“ in [^1]

[75] https://de.wikipedia.org/wiki/Agilit%C3%A4t_(Management)

selten Dateien und Ordner Leerzeichen, Unterstriche oder A-,AAA- oder AAAAA-Präfixe erhalten, damit sie im Windows-Explorer oben stehen.

Das verursacht in mir nicht nur Brechreize sondern ist zugleich fehleranfällig, unflexibel, nicht portabel und mit dem Makel klassischer Client-Server-Architekturen[76] behaftet: Der Letzte überschreibt immer den Versionsstand des Vorhergehenden. Ohne eine Versionsverwaltung können keine Äste und Gabelungen eines Projektverlaufes abgebildet, Datei- oder Verzeichnisstrukturen in Gänze immer übertragen werden. Das ist Gift für jeden mobilen Arbeitsplatz mit schwacher Internetverbindung.

Git, Gitea, UML & Nextcloud

Dabei nutze ich als Softwareentwickler mit git[77] eine bewährte Technologie. Der eigener Server ist mit Gitea[78] schnell aufgesetzt[79] und ermöglicht auch Nicht-Softwareentwicklern für Nicht-Softwareprojekte den einfachen Zugang via Web-Frontend. Einmal auf Markdown[80] und UML[81] als Dokumentenformat geeignet, entfallen auf einen Schlag alle Probleme mit proprietären, binären Dokumentenformaten.

Es muß aber nicht gleich git sein. Die rudimentäre Versionskontrolle einer Nextcloud[82] reicht auch. Hier gefallen die kurzen Wege zu spontanen Chats und Videokonferenzen mit Talk sowie die Integration mit weiteren kollaborativen Apps.

Selbstverständlich eignen sich zur Kommunikation auch Tools wie Mattermost[83] und andere, solange diese frei, selbst gehostet und ohne Datenabflüsse an Dritte sind. Weniger ist mehr! Der Golem-Artikel „An der falschen Stelle automatisiert“[84] fasst es in einem Satz zusammen:

---

[76] https://de.wikipedia.org/wiki/Client-Server-Modell

[77] https://git-scm.com/

[78] https://gitea.io/

[79] https://blog.jakobs.systems/blog/gitea-statt-github/

[80] https://de.wikipedia.org/wiki/Markdown

[81] https://blog.jakobs.systems/blog/gitea-uml-mermaid/

[82] https://nextcloud.com

[83] https://mattermost.com/

[84] https://www.golem.de/news/projektmanagement-an-der-falschen-stelle-automatisiert-1906-141628.html

> Wir schaden (…) der Produktivität und dem persönlichen Wohlbefinden, wenn wir ständig Trends nachlaufen und trotzdem nie wirklich auf dem neuesten Stand sein können.

Teams, Slack, Discord & Zoom sind ungeeignet

Tools wie Microsoft Teams, Slack, Discord, Zoom & Co sind aus meiner Sicht für ein Projektmanagement aus folgenden Gründen ungeeignet:

1. Es stehen schwerwiegende Sicherheitsvorfälle[85] und ungeklärte Datenschutzprobleme im Raum[86]. Die DSGVO ist das geringste Problem. Jemand möge mir bitte erklären, wie ich mit einer unterschriebenen und strafbewehrten NDA-Verschwiegenheitserklärung etwas in Projekten einsetzen kann, wo qua EULA und Datenschutzerklärung die Weitergabe und uneingeschränkte Unterlizenzierung zur Nutzung durch Dritte erfolgt?[87].
2. Keines der genannten Softwareprodukte löst das Problem der Langzeitarchivierung oder Compliance. Wie mit der GoBD[88] umgehen? Auf einen Nenner gebracht müssen Chatverläufe, Dokumente und Assets auch nach 6 oder 10 Jahren abrufbar bleiben. Proprietäre, unfreie Dateiformate oder Webdienste, die von Herstellern nach Gutdünken aufgegeben werden, stehen diesem Ansinnen diametral entgegen. Ein schönes Negativbeispiel hat unlängst die Unternehmensberatung KPMG gegeben. Chatverläufe inkl. Dateien von 145.000 Mitarbeitern waren mit einem Mausklick weg[89].
3. Die Geschäftsmodelle der Hersteller zielen auf einen Vendor Lock-in[90] bei stetig steigenden Kosten. Einmal mit einem Bein in einem solchen Ökosystem und im Verlauf der Zeit werden die „Spielregeln“ subtil und mit viel Nudging[91] verändert. Wichtige Funktionen

[85] https://www.heise.de/security/meldung/Videokonferenz-Software-Ist-Zoom-ein-Sicherheitsalptraum-4695000.html

[86] https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf

[87] http://blog.jakobs.systems/blog/20200905-privacy-shield-discord/

[88] https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/2019-11-28-GoBD.html

[89] https://www.golem.de/news/teams-kpmg-loescht-aus-versehen-chats-von-145-000-angestellten-2008-150457.html

[90] https://en.wikipedia.org/wiki/Vendor_lock-in

[91] https://de.wikipedia.org/wiki/Nudge

einer Software, die aus einer bestehenden „Pro“ Lizenz plötzlich in eine teurere, neugeschaffene „Enterprise“ Lizenz wandern gab es beim Wechsel von Win7 auf Win10. Das ist opportunistisches Ausnutzen einer Informationsasymmetrie[92]. George Akerlov mit seiner Todesspirale lässt grüßen[93].

Risiko-Algebra

Egal was am Ende einer Projektierung herausfällt, ohne Abstimmung mit einem ISB und der Informationssicherheit läuft nichts. Dabei muß nicht für alles eine aufwändige Risikoanalyse erstellt werden.

Ein Beispiel: Wenn ein Mitarbeiter daheim vom Arbeitgeber einen Rechner erhalten soll, der komplett außerhalb des Firmennetzes steht und lediglich Mails per Webmailer (mit 2FA) abruft, reicht der marktübliche Standard. Meinetwegen auch mit einer Lage Schlangenöl zum Wohlfühlen. Eine Systemhärtung und aufwändige Risikoanalyse ist bei so was Zeitverschwendung. Es gilt: Wo keine Gefährdung, da kein Risiko.

Wie wird dieses Beispiel beschrieben und visualisiert? Anhand der nachfolgenden Formel und einiger Hilfstabellen, die ich hier zum Download anbiete und vorstelle:

> **Risiko = Schadenspotential x Eintrittswahrscheinlichkeit**

Betrachten wir die maximal zu erwartende Schadenshöhe und merken uns die erreichte Punktzahl.

[92] https://de.wikipedia.org/wiki/Asymmetrische_Information

[93] https://de.wikipedia.org/wiki/George_A._Akerlof

Schadenshöhe	Wert	Geschäftsprozesse	Unternehmenswerte	Gefahr für Leib und Leben	Verstoß gegen Gesetze oder Verträge	Wiederherstellung
vernachlässigbar	1	Zentrale Geschäftsprozesse werden nicht gestört	Unternehmenswerte gehen nur in einem geringen Umfang verloren	Es besteht keine Gefahr für Leib und Leben	Es liegen keine Verstöße gegen Gesetze oder Verträge vor	Eine Wiederaufnahme kann im Rahmen des normalen Geschäftsbetriebes geleistet werden.
spürbar	2	Zentrale Geschäftsprozesse werden zwar gestört, die Störung ist jedoch nicht wesentlich	Unternehmenswerte gehen nicht in einem wesentlichen Umfang verloren	Es besteht keine Gefahr für Leib und Leben	Es liegt ein Verstoß gegen Gesetze oder Normen vor. Die daraus resultierende Haftung ist gering.	Der Schaden ist behebbar ohne daß wesentliche Mittel des Unternehmens eingesetzt werden müssen.
schmerzhaft	4	Der Schaden stört zentrale Geschäftsprozesse empfindlich oder bringt diese zum Erliegen	Es gehen wesentliche Unternehmenswerte verloren.	Es können Menschen verletzt werden.	Es liegt ein Verstoß gegen Gesetze oder Verträge vor. Die resultierende Haftung ist beträchtlich, jedoch nicht ruinös.	Der Schaden kann mit den Mitteln des Unternehmens behoben werden, bevor er den Bestand des Unternehmens unmöglich macht.
katastrophal	8	Zentrale Geschäftsprozesse werden zum Erliegen gebracht. Die Rückkehr zum Regelbetrieb ist innerhalb eines akzeptablen Zeitraumes nicht möglich.	Es gehen wesentliche Unternehmenswerte verloren oder werden zerstört. Eine Wiederherstellung ist nicht mehr möglich.	Es können Menschen schwer verletzt werden oder kommen ums Leben.	Gesetze und Verträge werden gebrochen und die resultierende Haftung für das Unternehmen/ Verantwortliche ist ruinös.	Der Schaden kann mit den Mitteln des Unternehmens nicht wieder behoben werden.

Abbildung 9: Tabelle Schadenshöhe

Jetzt wird es ein wenig schwieriger. Wir schätzen die Eintrittswahrscheinlichkeit. Hier gewinnt immer die Zeile, mit den meisten, zutreffenden Aussagen. Bitte auch hier die Punktzahl merken.

Wahrscheinlichkeit	Wert	Robustheit	Erfahrungswert	Einschätzung	Rahmenbedingungen
unwahrscheinlich	1	Das System arbeitet aktiv gegen den Eintritt des Ereignisses	In der Vergangenheit ist das Ereignis gar nicht oder nur sehr selten aufgetreten.	Der Eintritt des Ereignisses im betrachteten Zeitraum wäre eine Überraschung.	Das Ereignis kann nur eintreten, wenn spezielle Rahmenbedingungen gegeben sind, die im betrachteten Zeitraum sehr selten sind.
möglich	2	Das System ist vor dem Eintritt des Ereignisses geschützt, allerdings ist dieser Schutz nicht zuverlässig.	In der Vergangenheit ist das Ereignis schon aufgetreten.	Der Eintritt des Ereignisses wäre keine Überraschung.	Die Rahmenbedingungen für den Eintritt des Ereignisses können in der Praxis durchaus vorkommen.
wahrscheinlich	4	Das System verhindert den Eintritt des Ereignisses nicht.	Das Ereignis ist schon häufig aufgetreten.	Das Ereignis wird im betrachteten Zeitraum erwartet.	Die Bedingungen für den Eintritt des Ereignisses sind häufig oder sogar permanent gegeben.
sehr wahrscheinlich	8	Das System entwickelt sich zwangsläufig auf den Eintritt des Ereignisses zu.	In der Vergangenheit ist das Ereignis immer wieder aufgetreten, das Ereignis tritt regelmäßig auf oder ist akut.	Das Ereignis wird im betrachteten Zeitraum eintreten.	Die Rahmenbedingungen für den Eintritt des Ereignisses sind permanent gegeben.

Abbildung 10: Tabelle Wahrscheinlichkeit

Die beiden Zahlen multiplizieren und das Ergebnis vergleichen:

Wert	Risiko	Behandlung	Aufwand
1	sehr gering	Das Risiko sollte akzeptiert werden	Behandlung nur bei sehr wenig Aufwand
2-4	gering	Das Risiko kann akzeptiert werden	Behandlung nur bei wenig Aufwand
8	mittel	Das Risiko sollte behandelt werden	Behandlung nur mit moderatem Aufwand
16-32	hoch	Das Risiko muss behandelt werden	Behandlung auch bei hohem Aufwandnotwendig
64	sehr hoch	Das Risiko muss sofort behandelt werden	Behandlung auch bei sehr hohem Aufwandnotwendig

Abbildung 11: Tabelle Risikobestimmung

Ich komme in unserem Beispiel auf den Wert 2, geringes Risiko. Eingesetzt in einer farbigen Risikomatrix wird sofort sichtbar: Wir liegen im grünen Bereich.

	vernachlässigbar	spürbar	schmerzhaft	katastrophal
sehr warhscheinlich	mittel (8)	hoch (16)	hoch (32)	sehr hoch (64)
wahrscheinlich	gering (4)	mittel (8)	hoch (16)	hoch (32)
möglich	gering (2)	gering (4)	mittel (8)	hoch (16)
unwahrscheinlich	sehr gering (1)	gering (2)	gering (4)	mittel (8)

Abbildung 12: Tabelle Risikobestimmung

Diese Hilfstabellen erleichtern einem das Leben und geben Orientierung Risiken zu bewerten und entweder kompensierende Maßnahmen oder weitergehende Risikoanalysen zu erarbeiten.

Zuletzt ein Hinweis in eigener Sache:

> Ich bin für solche Digitalisierungsprojekte zu haben und bringe meine Expertise ein. Das macht mir sogar richtig Spaß egal ob kurzfristig als Problemlöser oder längerfristig als Coach, Mentor oder Projektleiter.

> Das neue Jahr 2021 steht bevor. Bitte rechtzeitig für Projekte in der Pipe ansprechen, damit wir gemeinsam ab Januar mit Volldampf loslegen können.

Änderungsverzeichnis

Update 23.08.2020

Veröffentlichung erster Teil

Update 30.08.2020

Veröffentlichung zweiter Teil

Update 16.10.2020

Veröffentlichung dritter Teil

Update 26.04.2021

Überschriften angepasst zur besseren Unterstützung von pandoc zum automatischen Erzeugen von PDF-Printouts. Änderungsverzeichnis am letzten Teil angehängt.