Digitale Forensik

Dipl.-Ing. Thomas Käfer, M.Sc.

5. Ausgabe

Updates? Nein Danke!
Da lass ich mich lieber hacken!

www.KaeferLive.de

DigiFor Inside 5. Ausgabe

Updates? Nein Danke!
Da lass ich mich lieber hacken!

Impressum

Herausgeber: KäferLive - Käfer IT Systeme e.K.
Elchenrather Weide 20
52146 Würselen
Tel. 02405/47949-0

Autor: Dipl.-Ing. Thomas Käfer, M.Sc.
Von der IHK Aachen Öffentlich bestellter und vereidigter Sachverständiger
für Systeme und Anwendungen der Informationsverarbeitung
Master of Science Digitale Forensik

Website: https://www.KaeferLive.de
E-Mail: service@KaeferLive.de

Bildnachweis: Quelle Fotolia.com bzw. eigene Aufnahmen/Grafiken (mit KI generiert)

Bezug und weitere Informationen und Artikel siehe:
https://www.kaeferlive.de

Erscheinungsdatum: Februar 2025

Danksagung

Besonderer Dank geht an meine Frau Michaela Käfer, die wieder die Qualitätskontrolle übernommen hat. Bei der akribischen Jagd auf Tippfehler ist sie natürlich wieder fündig geworden.

Inhalt

About DigiFor Inside

Was ist DigiFor Inside? DigiFor ist die Kurzform für den Begriff „Digitale Forensik“, einem Spezialgebiet der IT, welches sich mit der Analyse und Aufdeckung von Sicherheitsvorfällen (sogenannten Incidents) und missbräuchlicher Nutzung von Computern im Rahmen von Straftaten und zivilrechtlichen Auseinandersetzungen beschäftigt. DigiFor Inside ist eine Reihe von Fachaufsätzen und Veröffentlichungen, publiziert auf dem Portal KäferLive (https://www.KaeferLive.de), bei denen der Autor Thomas Käfer aus dem IT-Nähkästchen plaudert und Angriffskonzepte und Maßnahmen zu deren Erkennung bzw. Abwehr offenlegt.

Mit diesem Artikel möchte ich mich mit den Themen „Update“ und „Upgrade“ beschäftigen und beleuchten, was sie mit IT-Sicherheit zu tun haben. Da ich ja des Öfteren dazu neige, mit dem erhobenen Zeigefinger auf Missstände hinzuweisen bzw. selbige anzuprangern, mache ich auch vor diesem Thema nicht halt. Nicht um Sie zu quälen, sondern um zu zeigen, welchen Einfluss eine falsche oder gar vernachlässigte Updatepolitik auf IT-Security hat und welchen Gefahren man sich aussetzt, wenn man seine Systeme nicht zeitnah, sorgfältig und konsequent auf einem aktuellen Stand hält. Wie immer gibt es Beispiele aus der Praxis und eigene Erfahrungsberichte und hier wird es dann konstruktiv. Denn als Fach- und Romanautor muss man sich gelegentlich selbst an die Nase fassen und prüfen, ob die eigene IT noch auf der Höhe der Zeit ist oder ob auch hier der Spruch „Der Schuster hat die schlechtesten Schuhe“ gilt.

Also viel Spaß (oder auch nicht) bei der Lektüre.

Ihr Thomas Käfer

Übrigens: Wer sich für IT interessiert, aber das Thema lieber in einem unterhaltsamen Roman verpackt konsumieren möchte, dem sei mein neuer Krimi „Falk Zwo“ empfohlen, der keine 14 Jahre nach meinem Erstlingswerk „Praha“ am 20. Dezember 2024 veröffentlicht wurde.

About me

Ich bin mit meinem IT-Systemhaus seit 1990 selbstständig in der IT tätig. Das Tätigkeitsfeld der Firma Käfer umfasst Consulting-Leistungen im Bereich der IT-Sicherheit incl. Penetration-Testing u.a. im Automotive-Umfeld sowie die Entwicklung und der Vertrieb von Full-Motion-Simulatoren für Racing und Flight. Seit 2002 arbeite ich als Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung (seit 2006 öffentlich bestellt), als IT-Consultant, externer Datenschutzbeauftragter, Fachautor und beschäftigte mich vor allem mit Fragen der IT-Sicherheit, dem Datenschutz und dem Gebiet der Digitalen Forensik. Ehrenämter als Handelsrichter am Landgericht Aachen sowie als Mitglied der Vollversammlung der IHK Aachen (Ausschüsse Industrie und Technologie, Außenhandel sowie Berufsbildung) komplettierten in der Vergangenheit meine Tätigkeiten. 2015 habe ich aus „lauter Langeweile“ erfolgreich den berufsbegleitenden Masterstudiengang „Digitale Forensik“ an der Hochschule Albstadt-Sigmaringen in Kooperation mit der LMU München und der FAU Erlangen abgeschlossen und in diesem Rahmen eine umfangreiche Forschungsarbeit zum Thema Digitale Kfz-Forensik (Car-Forensics) erstellt. Ich bin Speaker auf Veranstaltungen zum Thema IT-Sicherheit und Datenschutz und halte Schulungen und Workshops zu diesen Themen für Automobilindustrie, Industrie, Zulieferern, Behörden und Verbände. Privat bin ich glücklich verheiratet, begeisteter Motorradfahrer und seit 2024 auch Inhaber einer Pilotenlizenz PPL(A) für einmotorige Motorflugzeuge. Die Begeisterung für Literatur und die Freude am Spiel mit dem gesprochenen und geschriebenen Wort spiegelt sich in vielen eher technisch und sachlich orientierten Publikationen und Schriftsätzen aber auch in den Kriminalromanen „Praha“ und „Falk Zwo“ wieder.

Motivation und Begriffsbestimmung

Never touch a running system!

Wer sich in seinem beruflichen Leben in den letzten Jahrzehnten mit EDV oder neudeutsch „IT“ beschäftigt hat, wird diesen Satz mehr als einmal gehört haben. Es ist sozusagen eines der IT-Gebote und warnt übereifrige System-Administratoren davor, Hand an ein funktionierendes System zu legen. Die bittere Erfahrung, die hinter diesem Leitsatz steht, ist die Erkenntnis, dass ein fragiles IT-Konstrukt den Betrieb einstellen kann, nachdem man an einer Komponente – mit den besten Absichten – etwas „optimiert“ hat.

Im Netz finden sich zahlreiche witzige Schaubilder zu diesem Thema, deren Message ist: „Lass die Finger davon“. Tatsächlich konnte man nach dieser Devise jahrelang seine IT betreiben. Wenn es einmal läuft, Finger weg. Und da die meisten Administratoren und Entwickler eine gute Dokumentation ihrer eigenen Arbeit scheuen wie der Teufel das Weihwasser, ist nach Jahren unangetasteten Daseins auch guter Rat teuer, wie denn dieses „Ding“ eigentlich funktioniert. Nicht mal die damaligen Urheber des Werkes wissen das nach einiger Zeit noch und die nachfolgenden Generationen stochern komplett im Nebel.

Das Prinzip „Never touch a running system“ ging aber nur so lange gut, wie diese Systeme isoliert in einer Nussschale und komplett gekapselt von der Außenwelt betrieben wurden. Das ist auch der Grund, warum man in vielen Industriesteuerungen total veraltete Betriebssysteme findet, die seit Jahrzehnten nicht mehr gepatched wurden – und das ist okay. Solange ein ICE keine Verbindung nach außen hat, kann man ihn problemlos mit Windows 3.11 betreiben[1]. Und auch in Fabrikhallen findet man noch genügend DOS oder Windows XP-Rechner, mit denen z.B. eine CNC-Maschine programmiert bzw. gesteuert wird. Solange diese Systeme in einem 100% gekapselten Netzwerk oder gar „Stand-Alone“ betrieben werden und funktionieren, gilt tatsächlich: Bloß nicht anrühren! Meist ist selbst der damalige Hersteller nicht mehr in der Lage, die Systeme zu aktualisieren oder es handelt sich um eine Eigenprogrammierung eines Mitarbeiters, der längst in Rente gegangen ist. So oder so gibt es meist keine belastbare Dokumentation und so traut sich zu Recht niemand, solch ein System auf den aktuellen Stand der Technik zu bringen. Solange die Maschine nicht mit der Außenwelt kommunizieren muss und kein Bedarf für funktionale Erweiterungen besteht, ist ein Update oder Upgrade auch nicht nötig.

Wenn aber dann doch der Wunsch der Geschäftsführung kommt, den Maschinenpark vom Tablett aus zu steuern oder direkt mit dem ERP-System zu koppeln, führt kein Weg an einem Upgrade vorbei. Einfach nur das Netzwerkkabel der Industriesteuerung (OT) in das Office-Netz zu stöpseln, führt unweigerlich ins Verderben. Also muss ein Update oder Upgrade her!

[1] Quelle Heise: https://www.heise.de/news/Deutsche-Bahn-sucht-Admin-fuer-Windows-3-11-for-Workgroups-9611543.html

Update vs. Upgrade

Ist das nicht ein- und dasselbe? Nicht ganz. Unter „Updates“ versteht man Aktualisierungen primär von Software, die in der Regel keine wesentlichen Funktionserweiterungen liefern, sondern Fehlerbehebungen oder Anpassungen auf geänderte Betriebsumgebungen, zum Beispiel bei Anwendungssoftware, die auf einer neuen Betriebssystemversion lauffähig gemacht wird. Ein weiteres Merkmal ist, dass Updates meist kostenfrei zur Verfügung gestellt werden und die Frequenz von Aktualisierungen höher liegt als bei Upgrades.

Ein Upgrade hingegen ist meistens bzw. eher kostenpflichtig, kennzeichnet sich durch einen größeren Versionssprung und liefert oft eine Erweiterung bzw. Veränderung des Funktionsumfangs.

Und dann gibt es noch Bugfixes und Patches. Während ein Bugfix manchmal eine mit heißer Nadel gestrickte Fehlerbehebung ist (wahrscheinlich daher auch die Bezeichnung „Hotfix“ für besonders dringende Aktualisierungen), versteht man unter einem Patch schon einen richtigen „Flicken“, der auf die löchrige Jeans genäht wird, damit sie noch ein paar Schlammschlachten mehr durchhält, bevor sie auseinanderbröselt.

Updates fassen meist mehrere Bugfixes und Patches zusammen und bessern eine Software so nach, dass sie – bis zum nächsten gefundenen Fehler – weiter betrieben werden kann.

Und hier stoßen wir bereits auf eine wesentliche Eigenschaft von Software, die sie von Hardware unterscheidet: Hardware kann kaputt gehen – Software ist grundsätzlich defekt. Dieser Spruch ist mittlerweile auch herrschende Rechtsauffassung an Gerichten, denn es ist nahezu unmöglich, fehlerfreie Programme zu entwickeln. Sobald man ein Programm schreibt, das nur unwesentlich von dem Code { } abweicht, sind Bugs vorprogrammiert.

Wie ich nun genau auf den Code { } komme und was dahinter steckt? Die Antwort gibt der bereits in der Einleitung erwähnte Roman „Praha“.

Gemäß einem Vortrag der BSI-Chefin Claudia Plattner auf dem NRW-IT-Sicherheitstag in Bonn im Dezember 2024 werden täglich 78 neue Schwachstellen in Softwareprodukten gefunden. Pro Tag kommen durchschnittlich 309.000 Schadprogramm-Varianten „auf den Markt“ und es werden ebenfalls täglich rund 1.000 neue Phishing-URLs und -IPs entdeckt. Und diese Entwicklung ist sehr dynamisch: Laut BSI nahm die Zahl der global pro Tag bekannt gewordenen Schwachstellen von 2022 auf 2023 um 14% zu und das BSI verzeichnete eine Zunahme von gemeldeten Cyber-Vorfällen um 33%. Nach einer Bitkom Studie entstanden allein im Jahr 2024 rund 179 Milliarden Euro Schaden durch Cyber-Angriffe bei deutschen Unternehmen[2].

Eine Gegenmaßnahme sind zeitnah aktualisierte Systeme. Aber auch das kann fürchterlich schief gehen. Sie werden sich sicherlich noch an den CrowdStrike Vorfall am 19. Juli 2024 erinnern.

[2] Quelle: https://www.bitkom.org/Presse/Presseinformation/10-Milliarden-Euro-Deutschlands-Cybersicherheit

Da stand die Welt für einen Tag quasi still, weil durch ein fehlerhaftes und offenbar nicht oder unzureichend getestetes Update rund 8,5 Millionen Computer weltweit in eine sogenannte Blue Screen of Death-Schleife (BSOD) gerieten. Der weltweite Schaden belief sich auf geschätzt mindestens 5 Mrd. USD. Manche Quelle geht sogar von einer Summe von rund 15 Mrd. USD aus[3]. 40% der direkt betroffenen Unternehmen konnten ihre Leistungen teilweise für mehrere Tage nicht erbringen[4].

Besonders bitter: CrowdStrike ist ein Anbieter von Endpoint-Protection-Lösungen, also Software, die den Computer sicherer machen soll. Eigentlich sollte die Software also die Betriebssicherheit sicherstellen, hat aber die Systeme leider unbrauchbar gemacht, so wie bei einem klassischen Hacker-Angriff.

Und hier zeigt sich an einem prominenten Beispiel das Spannungsfeld, in dem wir uns bewegen. Einerseits war seitens CrowdStrike offenbar höchste Eile geboten, da man auf eine neuartige Bedrohungslage reagieren wollte und andererseits hätte Sorgfalt vor Schnelligkeit den tatsächlichen Schaden womöglich deutlich reduziert.

Denn auch das ist eine bittere Wahrheit. Windows-Nutzer bekommen seit Jahren mindestens einmal pro Monat neue Windows-Updates. Meist werden diese am sogenannten Patch-Tuesday ausgerollt. Das ist der zweite Dienstag im Monat. Dieser feste Termin ist etabliert und zeigt, dass es selbst einem Software-Giganten wie Microsoft nicht gelingen will, wenigstens für den Zeitraum von mehr als einem Monat fehlerfreie Software auszuliefern. Wohl gemerkt handelt es sich bei den Updates, die an diesem Tag bereitgestellt werden, in der Regel nicht um Funktionserweiterungen, sondern um reine Bugfixes bzw. Reaktionen auf neu bekannt gewordene Schwachstellen bzw. Angriffsvektoren.

Updates first!

Dass die Devise „Never touch a running system“ nicht mehr aufgeht, haben wir besprochen. Also machen wir jetzt konsequent und zeitnah die Updates? Ja und nein.

In der Zeit, als ich mit meinen Mitarbeitern noch klassischen IT-Service betrieben habe, war einer der ersten Checks bei einem vom User gemeldeten Problem, ob vielleicht gerade Updates installiert wurden oder in der aktuellen Windows-Session als Download angeboten werden. Streikte auf einmal ein Drucker, ohne dass es dort eine bewusste Veränderung gegeben hatte, lag der Verdacht nah, dass es mit einem Windows-Update zu tun haben könnte. Oft war das genau der Fall und entweder gab es vom Druckerhersteller dann kurz danach ein Treiber-Update oder man wartete einfach auf den nächsten Patch-Tuesday und der Fehler vom letzten Monat wurde wieder ausgemerzt – natürlich nicht ohne wieder neue Fehler und Wechselwirkungen an anderer Stelle einzubauen.

Andererseits haben wir viele Fehler einfach dadurch behoben, dass wir alle zur Aktualisierung anstehenden Updates eingespielt haben. Woran die Fehlfunktion dann genau lag, haben wir nie herausgefunden. Das hätte extra Geld gekostet. Wichtig (für den Kunden) war, dass das System danach wieder lief. Auch ein gerade in der Installation befindliches Update konnte schon einmal für unerwünschte Effekte sorgen. Dann ließ man einfach das Update durchlaufen und den Rechner neu starten. Meist war dadurch das Problem verschwunden. Übrigens werden etwa 50% aller IT-Probleme allein durch einen Neustart „behoben“.

Eine andere Vorgehensweise für die Fehlersuche ist, den Kunden / User zunächst zu fragen: „Was haben Sie gemacht / verändert?“ Die Standard-Antwort ist: „Nichts“.

---

[3] Quelle Neowin: https://www.neowin.net/news/systems-paralyzed-by-crowdstrike-within-78-minutes-to-cause-15-billion-in-losses-worldwide/

[4] Quelle BSI: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/240919_BSI-bitkom_Crowdstrike-Umfrage.html

Die Nachfolgefrage „Und was haben Sie gemacht, bevor sie *nichts* gemacht haben?“ bringt dann meist Licht ins Dunkle. Oft wurde „nur“ ein neues Programm oder eine neue Programmversion installiert. In aller Regel sind Windows-Updates aber ein Segen. Durch die enorme Verbreitung von Microsoft-Produkten kann man davon ausgehen, dass man mit seinem konkreten Problem nicht der einzige auf der Welt ist und es bereits eine Abhilfe gibt (Google ist Dein Freund!). Und so werden durch die Windows- und Office-Updates in der überwiegenden Zahl der Fälle Probleme gelöst, bevor sie einen Impact haben und ersparen dem Anwender eigene Abhilfeversuche. Manchmal geht auch ein Windows-Update gehörig in die Hose. Dann funktioniert im schlimmsten Fall der Rechner nicht mehr und muss neu installiert werden. Hat man ein aktuelles Backup, ist auch das zu verschmerzen und man setzt in diesem Fall die Updates nach dem System-Restore für einige Zeit aus, bis fehlerbereinigte Versionen zur Verfügung stehen. Aber das darf dann eben nicht die dauerhafte Lösung sein!

Backup first!

Damit sind wir bei dem nächsten wichtigen Thema: „Backup“. Wie wir gelernt haben, ist Software grundsätzlich defekt bzw. kann kaputt gehen. Natürlich kann auch Hardware kann den Geist aufgeben und bei einer Festplatte ist nie die Frage, ob sie ausfällt, sondern wann. Tatsächlich haben moderne Festplatten eine erstaunliche Lebensdauer und ein Ausfall kommt oft nicht einmal ohne Vorwarnung. Egal ob Hardware-Defekt, ein Programmfehler oder eine Hacker-Attacke: Ohne ein einigermaßen aktuelles Backup ist der Tag versaut, wenn das System plötzlich steht.

Einen Rechner „from scratch“ wieder hochzuziehen ist schnell erledigt und eine Sache von ein bis drei Stunden. Der Teufel steckt – wie so oft – im Detail. Bis die Konfiguration wieder so ist, wie sie vorher war, alle Programme laufen und Verknüpfungen zu anderen Systemen wieder hergestellt sind, vergehen noch ein paar Stunden (oder Tage) mehr. Die selbst generierten bzw. gesammelten Nutzer-Daten kann jedoch kein System-Admin einfach wieder herzaubern. Die sind weg, wenn die Festplatte den Geist aufgegeben hat oder der Hacker alles verschlüsselt hat. Jetzt hilft nur ein aktuelles und vollständiges Backup und das ist bares Geld wert. Das ist nicht einmal bildlich gemeint. Wurden Sie Opfer eines Hackerangriffs und Ihre Daten sind verschlüsselt, dann fordern die Angreifer meist einen Betrag im fünf- oder sechsstelligen Eurobereich für den Key zur Entschlüsselung. Die laut dem Bundeslagebild Cybercrime im Jahr 2023 durchschnittlich gezahlte Lösegeldsumme lag bei 621.858 USD[5]. Liegt kein aktuelles Backup vor, bleibt Ihnen nur die Zahlung des Lösegelds, um wieder an Ihre Systeme und Daten zu kommen. Aber auch die Zahlung des Lösegelds ist kein Garant dafür, dass nachher wieder alles gut ist. Oft sind bei der Verschlüsselung Dateien korrumpiert worden und können nicht mehr wiederhergestellt werden. Und es versteht sich doch von selbst, dass nach der Entschlüsselung umgehend erheblicher Aufwand betrieben werden muss, um die Angreifer dauerhaft aus dem Netz auszusperren, denn warum sollten sie oder andere es nicht ein zweites Mal über dieselbe Schwachstelle versuchen. Dazu später mehr. Auch wenn man nicht Opfer einer Hackerattacke geworden ist, rettet ein Backup. Wenn nämlich besagter Fall eintritt und ein Windows- oder Programm-Update dazu führt, dass der Computer nicht mehr oder nicht vollständig startet, kann der Rollback auf den letzten funktionierenden Stand die Rettung sein. In virtualisierten Umgebungen macht man dazu vor jeder Systemänderung im laufenden Betrieb einen Snapshot, auf den man das System nach der Änderung sofort wieder zurücksetzen kann (zeitnahe Konsolidierung der Snapshots und Patchen der Host-Umgebungen selbst nicht vergessen!). Bei Bare-Metall-Systemen geht das genauso, denn Windows bietet neben der System-wiederherstellungsfunktion bei Server-Betriebssystemen auch die sogenannte Windows-Server-Sicherung. Hat man beispielsweise in einem Kleinbetrieb nur einen Server ohne Virtualisierung, kann man mit der auf Wunsch automatisiert laufenden Server-Sicherung ein vollständiges Abbild generieren, welches bei Bedarf bei einem nicht mehr startenden System über die Reparaturoptionen im Bootmanager zurückgespielt werden kann. Dann sind „nur“ die Änderungen zwischen letztem Backup und dem Zeitpunkt des Zurückspielens verloren.

[5] Quelle: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2023.pdf?__blob=publicationFile&v=5

Hat man die System- von den Datenpartitionen getrennt, ist das noch nicht mal ein Problem, denn man setzt nur das Betriebssystem zurück. Die Daten bleiben unangetastet, werden separat gesichert und sind bei einem Betriebssystem-Defekt oft gar nicht betroffen.

Eigentlich unnötig zu erwähnen ist, dass ein Backup auch defekt sein kann. Nach Murphy betrifft es immer das Backup, welches man am dringendsten braucht. Der kluge Mensch baut daher vor und hat mehrere Versionen seiner Datensicherungen, die sich sowohl durch die Versionierung und Sicherungszeitpunkt als auch durch ihren Ablageort unterscheiden. Ideal sind kombinierte Backups auf verschiedenen Systemen und Medienarten z.B. Festplattenbackups in mehreren Versionen und ausgelagerte Sicherungen auf Tapes oder Wechseldatenträgern bzw. in der Cloud. Dann kann man selbst einen Daten-GAU abwenden und findet vielleicht in der 2. oder 3. Version eine brauchbare Kopie der Daten. Wichtig ist hierbei, dass ein Angreifer, der sich im System eingenistet hat, nicht an das Backup herankommen kann. Das ist nämlich eine der ersten Maßnahmen, die ein pfiffiger Hacker durchführt: Erst Daten abziehen (zur späteren Erpressung), dann das Backup zerstören und erst danach die Systeme verschlüsseln. So rollt der Rubel (für den Hacker) mit großer Wahrscheinlichkeit, denn mit einem kaputten Backup gehen einem Opfer die Optionen aus.

Haben wir aber alles richtig gemacht und sind durch funktionierende Backups gewappnet, können wir uns also an die Updates oder Upgrades herantrauen.

Update-Frequenz und Zeitpunkt

Wann ist nun der richtige Zeitpunkt, Updates einzuspielen? Man sollte sich vom Grundsatz leiten lassen: „So spät wie möglich – so schnell wie nötig“. Ist das ein Widerspruch zu den voran ausgeführten Gedanken?

So schnell wie nötig: Bei sicherheits-relevanten Updates ist Zeit der entscheidende Faktor. Nur wenn der Virenscanner die Bedrohungslage kennt, die ihn sehr bald ereilen wird, kann er reagieren. Daher sind Sicherheits-Updates und Aktualisierungen für Virensignaturen und Endpoint-Schutz mit Priorität so schnell wie möglich zu installieren und auszurollen – hoffentlich dann mit mehr Sorgfalt geprüft als beim CrowdStrike-Vorfall.

So spät wie möglich: Um nicht unnötigerweise Opfer eines unzureichend getesteten oder inkompatiblen Updates oder Upgrades zu werden, empfiehlt es sich wiederum, nicht bei den ersten dabei zu sein, wenn es um nicht-sicherheitskritische Aktualisierungen geht. Installiert man diese mit ein paar Tagen Verzug zum Patch-Day, dann sind offensichtlich fehlerhafte Updates wieder zurückgezogen worden bzw. es gibt dazu bereits passende Ergänzungen im Bereich Anwendungs-Software, Treiber oder Drittanbieter-Tools sowie das Know-how bei Tante Google, wie man bekannte Probleme löst.

Der Betrieb eines WSUS-Servers kann bei entsprechend großen Systemumgebungen übrigens eine Lösung sein, um Updates zunächst in geschützten Umgebungen auf Kompatibilität zu prüfen und erst nach Freigabe durch die eigene IT-Administration im gesamten Netzwerk auszurollen. Hier ergibt sich neben dem Download-Vorteil (Software muss nur einmal von externen Quellen geladen werden) die weitere Sicherheitsstufe, dass bestimmte Updates explizit (wegen Inkompatibilität) ausgeklammert und auf die Vertrauenswürdigkeit geprüft werden können. Nicht zu unterschätzen ist jedoch der Mehraufwand für derartige Prüfungen. Das macht nur Sinn, wenn es sich um große Umgebungen mit sehr homogenem Software-Umfeld handelt, da man hierbei einen großen Synergievorteil hat. Bei heterogenen Umgebungen oder Kleinbetrieben ist das Verfahren eher unter der Rubrik „mit Kanonen auf Spatzen geschossen“ abzuhaken. Zudem darf ein zwischengeschalteter WSUS-Server nicht dazu führen, dass nachher gar keine Updates oder nur sehr verzögert bei den Endgeräten ankommen. Ist der WSUS-Server nämlich selbst schlecht gewartet oder gar aus dem offiziellen Hersteller-Support herausgefallen, ist er ein eigenes Sicherheitsrisiko.

EOL-Systeme

EOL – also End-of-Life – ist das nächste wichtige Stichwort. Betriebssysteme und auch Anwendungs-Software unterliegen einem Lebenszyklus von der Entwicklung über die Veröffentlichung von Alpha- und Betaversionen hin zu der „fertigen“ Auslieferversion und der dann folgenden Maintenance-Phase, in der es Aktualisierungen gibt. Diese Wartungsphase dauert nicht ewig, sondern ist mittlerweile von den großen Herstellern klar definiert. Innerhalb des Lebenszyklus von Software gibt es unterschiedlich zugesicherte Verfügbarkeitszeiträume für diverse Levels von Updates[6]. I.d.R. wird beispielsweise bei Microsoft ein Produkt fünf Jahre nach Erscheinen im *Allgemeinen Support* betrieben, d.h. es gibt vollumfängliche Unterstützung bei Supportfällen (kostenlose und bezahlte Unterstützung bei Supportfällen, stündlich abgerechneter Support, Support für Garantieansprüche), Support mit Sicherheitsupdates und die Möglichkeit, nicht sicherheitsrelevante Updates anzufordern. In der darauffolgenden Phase des *Erweiterten Supports* gibt es für einige Produkte nur noch bezahlten Support und reine Sicherheitsupdates ohne zusätzliche Kosten.

Bei Desktop-Betriebssystemen gilt[7]: Während des erweiterten Supports stellt Microsoft weiterhin Softwareupdates für Sicherheit und Zuverlässigkeit sowie Fehlerbehebungen bereit. Nicht sicherheitsrelevante Updates werden jedoch ohne eine kostenpflichtige Support-Vereinbarung nicht bereitgestellt.

Daten und Fakten

Der Support für Windows 10 endet am 14. Oktober 2025. Der Support für Windows 8 endete am 12. Januar 2016, der für Windows 7 war am 14. Januar 2020 Geschichte und Windows 8.1 wird seit dem 10. Januar 2023 nicht mehr unterstützt. Das heißt, dass mit Stand Februar 2025 Windows 10 kurz vor seinem Betriebsende steht und nur noch Windows 11 als aktuell unterstütztes Betriebssystem für den Desktop gilt. Auch wenn Microsoft manchmal Ausnahmen macht, gibt es nach dem Support-Ende keine Sicherheitsupdates mehr und der Betrieb eines solchen EOL-Systems verbietet sich, sofern das System nicht vollständig von der Außenwelt abgeschirmt ist! Analog gilt das für Office-Versionen: Der Support für Office 2016 und Office 2019 endet am 14. Oktober 2025. Frühere Versionen gehören also sofort in den Müll.

Bei den Server-Produkten gilt ähnliches. So ist der Windows Server 2019 am 09.01.2024 aus dem Mainstream Support gefallen. Der Extended Support läuft noch bis zum 09.01.2029. Für alles ab Windows Server 2012 und darunter sieht es bereits seit Oktober 2023 düster aus. Hierfür gibt es keinerlei Updates mehr und ein Betrieb dieser Server ist grob fahrlässig. Dennoch sehe ich vor allem bei Incident Response Fällen (also, wenn die Hütte bereits lichterloh brennt) immer noch Windows 2008R2-Systeme – teils mit Exchange 2010 OnPrem im Produktiveinsatz. Da kann man dann nur sagen: No Mercy & No Compassion!

Die derzeit noch als aktuell geltende Version Server 2022 ist bis zum 13.10.2026 im Mainstream-Support und der Extended Support wird bis zum 14.10.2031 laufen.

Seit November 2024 gibt es nun die neueste Version Server 2025. Hier wird der Mainstream-Support bis zum 09.10.2029 und der erweiterte Support bis zum 10.10.2034 laufen. Investiert man jetzt also in ein Upgrade auf Windows Server 2025, hat man (Stand Februar 2025) die nächsten neun Jahre Ruhe (siehe dazu auch das nachfolgende Kapitel Beispiel Windows). Die gute Nachricht: So ein In-Place-Upgrade funktioniert oft auf Anhieb im laufenden Betrieb.

---

[6] Vgl. z.B. Microsoft: https://learn.microsoft.com/de-de/lifecycle/policies/fixed

[7] Quelle: Microsoft: https://support.microsoft.com/de-de/office/was-das-ende-des-supports-von-windows-f%C3%BCr-office-und-microsoft-365-bedeutet-34e28be4-1e4f-4928-b210-3f45d8215595

Wartungsfenster

Viele tief ins Betriebssystem eingreifende Updates und Upgrades bedingen vielfach einen Neustart des Systems. Das gilt nicht nur für Windows-Server sondern auch für Linux-Systeme und Hardware wie Router, Switche usw.. Hat das Unternehmen einen klassischen 9-to-5-Arbeitstag, findet sich meist problemlos ein Wartungsfenster am Abend oder Wochenende. Dummerweise geht der Trend aber mehr in Richtung 24/7-Betrieb und Systeme müssen jeden Tag rund um die Uhr laufen und das an 365 Tagen im Jahr. Damit sind Updates, die einen Neustart auslösen, praktisch ausgeschlossen.

Sollten Sie jetzt sagen: „Ja, das ist bei uns so“, dann haben Sie einen entscheidenden Denk- und Konfigurationsfehler bei Ihrer IT gemacht.

Kein System läuft zu 100% und kein professioneller Dienstleister wird Ihnen eine Verfügbarkeit von 100% anbieten oder garantieren. Tatsächlich arbeitet man bei der Verfügbarkeit mit dem 9er-System. Eine Verfügbarkeit von 99% bedeutet im Jahresmittel, dass das System in Summe knapp vier volle Tage nicht zur Verfügung steht (also 88 Stunden). Bei 99,9% reden wir über eine Verfügbarkeit mit einem Wartungsfenster von insgesamt knapp 9 Stunden im Jahr. Bei 99,99% stehen nur noch 53 Minuten p.a. zur Wartung zur Verfügung. Eigentlich unnötig zu erwähnen, dass jede 9er Stelle nach dem Komma immer mehr ins Geld geht.

Ein System mit einer Verfügbarkeit von mehr als 99% kann man ohne entsprechende Redundanzen überhaut nicht mehr betreiben. Hierbei wird ein Server auf ein weiteres System so gespiegelt, dass man immer eine Maschine außer Betrieb nehmen kann, um sie zu patchen oder zu reparieren, während das andere System den Betrieb aufrechterhält. Neben der doppelten Hardware und Software-Lizenzkosten kommen meist weitere Aufwendungen für die Steuerung des sogenannten High-Availability-Clusters (HA) hinzu.

Entweder verabschiedet man sich also von der Idee und Forderung einer nahezu hundertprozentigen Verfügbarkeit und schafft regelmäßige ausreichend dimensionierte Wartungsfenster für das Patchen von Systemen oder man investiert in eine HA-Lösung, um den Betrieb (nahezu) ausfallsicher zu machen.

Eine HA-Lösung nimmt den Druck vom Update-Kessel, denn die IT-Administratoren sind nicht mehr gezwungen, die Systemupdates am Wochenende oder in der Nacht in einem engen Zeitfenster durchzuprügeln, sondern können zu regulären Arbeitszeiten und mit der nötigen Ruhe die Server warten. Schlägt ein Update fehl, ist der Betrieb durch das weiterhin laufende Redundanzsystem gesichert und man kann sich mit der Fehlersuche und Behebung beschäftigen und anschließend einen erneuten Anlauf wagen. Das nimmt den Schrecken vor den Updates.

Natürlich ist auch eine HA-Lösung kein Selbstläufer, kann auch defekt gehen und ist alles andere als eine trivial zu installierende IT-Lösung, aber dafür gibt es Profis, die sich damit auskennen. Faktisch nutzt man diese Technik, wenn man sich in die Hände eines professionellen Cloud-Dienstleisters begibt, denn der wird seine virtualisierte Umgebung im Hintergrund schon aus Eigenantrieb redundant und auf aktuellem Niveau halten. Dann hat man mit dem Patchen direkt nichts mehr zu tun und es ist allein eine Frage des Geldes, wie hoch die zugesicherte Verfügbarkeit ist (s.o.).

Beim Patchen bitte auch Dritt-Anbieter- bzw. Anwendungs-Software wie Browser, Tools usw. nicht vergessen. Auch diese Programme sind voller Bugs und beliebtes Einfallstor für Schadcode.

Ab in die Hölle

Was passiert, wenn man EOL-Systeme weiterbetreibt oder Systeme nicht zeitnah patcht? Dann geht es ohne Umweg in die Hölle. Die Frage ist nicht, ob man heutzutage von bösen Buben angegriffen wird, sondern wann ein Angriff erfolgreich ist. Wie eingangs erwähnt, kommt jeden Tag eine Unmenge an neuen Schadcode-Varianten in Umlauf und die Hacker sind weit über ihr Garagen-Business hinausgewachsen und haben sich professionalisiert.

Es handelt sich um weltweit agierende Organisierte Kriminalität mit arbeitsteiligen Strukturen, Werkzeugen und hochqualifizierten Spezialisten. Das Geschäft ist extrem lukrativ und man munkelt, dass der Umsatz mit Cyber-Crime weltweit längst den mit Drogen übertroffen hat. Der Vorteil liegt auf der Hand: Cyber-Erpressung ist viel ungefährlicher als Drogenhandel und es sterben auch nicht so viele Kunden weg. Im Gegenteil: Jeden Tag kommen neue Kunden hinzu und manches Opfer wird auch nach einer Attacke nicht schlau und macht dieselben Fehler, die zum ersten Hack geführt haben, gleich wieder. IT und vor allem IT-Security ist Chef-Sache und anstatt sich immer wieder darüber zu beklagen, dass IT und Computer so viel Geld kosten, sollte sich mancher Unternehmer mal fragen, worauf denn sein Geschäftsmodell fußt. Ist das eigene Business ohne IT denkbar? Was kostet es, wenn das Unternehmen eine Stunde, einen Tag oder einen Monat nicht produzieren kann oder seine Dienstleistungen nicht mehr an Mann oder Frau verkaufen kann? IT ist eben nicht nur Kostenfaktor, sondern Enabler für so ziemlich jedes moderne Geschäftsmodell.

Ein Beispiel: Jeder Spediteur wird uns den Preis einer neuen Sattelzugmaschine auf den Euro genau sagen können und vorrechnen, wieviel Geld er pro Kilogramm Fracht fakturieren muss, damit er seine Speditionsaufträge wirtschaftlich und mit ausreichendem Gewinn abwickeln kann. Zu den 130.000,00 € für einen neuen Sattelzug kommen aber dummerweise noch die Kosten für die IT und deren Sicherheit on top, denn ohne funktionierende IT wird man sicher noch einen LKW durch die Gegend schicken können, bei 100 LKW und komplexen Speditionsverfahren wird es aber eng. Nach einem Tag ohne IT stehen alle Laster auf dem Rastplatz oder auf dem Hof still.

Daher gehören in eine ordentliche und belastbare Businesskalkulation nicht nur die Personal- und Raumkosten oder die Anschaffungskosten für das IT-Equipment, sondern zusätzlich sämtliche Lizenz- und Betriebskosten zur Aufrechterhaltung eines sicheren IT-Betriebs. Neben einem ausreichend starken und gut ausgebildeten IT-Team benötigt man eben auch aktuelle Hard- und Software.

Kleiner Side-Note: Software kann man oft sehr leicht einfach kopieren und ohne Lizenz betreiben. Das kann heftig ins Auge gehen und beschert uns Sachverständigen manchmal spannende Aufträge mit Gerichtsvollziehern, wenn wir mit großem Besteck mit einer einstweiligen Verfügung im Auftrag eines Landgerichts im Morgengrauen bei einem mutmaßlichen Lizenzbetrüger aufschlagen. Das wird richtig teuer, denn Software illegal zu nutzen, ist praktisch das gleiche, wie sich den benötigten Dienstwagen einfach vom Parkplatz des Autohauses zu stehlen (nach dem Motto: Wir haben da schon so viele gekauft und die haben noch so viele – das fällt in der Masse ja gar nicht auf).

Zurück zum Thema: Geradezu haarsträubend ist es, wenn man in Produktivumgebungen heutzutage immer noch Windows 2008R2-Server in Kombination mit einem Exchange Server 2010 on Premise findet. Ist es dann noch überraschend, wenn solche Systeme erfolgreich gehackt werden? Nein. Spätestens mit dem Hafnium-Schadcode war klar, dass es auch Application-Server im großen Stil treffen kann. Im Januar 2021 wurden weltweit hunderttausende Exchange-Server angegriffen und viele davon erfolgreich übernommen[8]. Das lag vor allem daran, dass Microsoft zu spät auf Hinweise von Sicherheitsforschern reagierte, die die Lücke im Dezember 2020 an den Hersteller gemeldet hatten und dann auch noch das nötige Update wegen fehlender Systemvoraussetzungen vielfach nicht sofort eingespielt werden konnte. Was seinerzeit schon eine Tragödie war (BSI: Alarmstufe ROT), lässt einen bei nachfolgenden Infektionen der Systeme im Herbst 2021 oder gar 2024 nur noch staunen. Da wurden Produktivsysteme mit dem Argument nicht gepatched, dass man schon mal schlechte Erfahrungen mit einem CU (Cumulative Update) auf einem Exchange gehabt habe und dieser danach nicht mehr funktioniert hätte oder man schlicht und einfach kein Zeitfenster gefunden hatte, die Maschinen auf einen aktuellen Stand zu bringen. Wir reden hierbei wohlgemerkt von Monaten bzw. Jahren, in denen solche Systeme ungepatched weiter betrieben wurden. Ohnehin war der Betrieb der Systeme auch im Jahr 2021 schon aus Sicherheitssicht unzulässig, da der Support bereits im Vorjahr beendet worden war. Der Hotfix von Microsoft auch für diese alten Systeme war damit nur Goodwill. Spätestens da hätte man die Entscheidung zu einem Upgrade treffen müssen.

---

[8] Quelle heise.de: https://www.heise.de/news/Der-Hafnium-Exchange-Server-Hack-Anatomie-einer-Katastrophe-5077269.html

Während diese Abhandlung entstanden ist, musste die Arbeit daran übrigens unterbrochen werden, weil ein aktueller Incident eines neuen Opfers abzuarbeiten war. Und was soll ich Ihnen sagen: Auch dieser Kunde hatte noch mehrere 2008er und 2012er Server im Einsatz. Nun ging es darum, diese Systeme in der Krise, d.h. im laufenden Incident, so schnell wie möglich auf einen ge-patchten Stand zu bringen, da zunächst unklar war, wie weit die Angreifer bereits in das OnPrem-Netz gedrungen waren. Was vorher über Monate – um nicht zu sagen Jahre – verschleppt wurde, erfolgte nun in zwei Tagen: InPlace-Upgrades von 2008 auf 2012 und dann von 2012 auf 2025. Das hätte man auch stressfrei und kostengünstiger haben können.

Zurück zum eigentlich geplanten Text: Die Hölle in diesen Beispielen bestand bzw. besteht darin, dass die Unternehmen erfolgreich gehackt wurden/werden und nicht unerheblich Geld ausgegeben haben bzw. werden, um die Folgen des Angriffs zu kompensieren. Hinzu kommen die ohnehin nötigen Investitionen in eine neue IT-Infrastruktur und der Umsatzausfall – vom Reputationsverlust und der persönlichen Gemütslage ganz zu schweigen. Ob übrigens eine Cyber- oder Betriebsunterbrechungs-Versicherung für den Schaden vollumfänglich eintritt, ist ein ganz anderes Thema. Wer bei Betrieb und Absicherung seiner IT-Infrastruktur grob fahrlässige und handwerkliche Fehler oder in den Fragebögen der Versicherer unwahre Angaben zur vermeintlichen IT-Security gemacht hat, geht im Schadenfall schnell leer aus. Ein von der Versicherung gestellter Forensiker hat beim Incident Response nicht selten den Auftrag, herauszufinden, ob es ggf. Vorschäden gab, die die Kompromittierung erst ermöglicht haben. Aber das ist schon wieder ein anderes Thema.

Übrigens: Die Folgen eines massiven Security-Incidents sind vielfach existenzbedrohend. Es gibt genügend prominente Beispiele in Deutschland, bei denen Unternehmen an den Rand und sogar in die Insolvenz getrieben wurden. Manche sprechen von bis zu einem Drittel der gehackten Unternehmen, die sich anschließend nicht mehr von dem Anschlag erholen. Bis so ein Verschlüsselungsangriff komplett abgearbeitet ist, vergehen typischerweise mindestens zwischen drei und sechs Monate, in vielen Fällen dauert es mehrere Jahre, bis die gesamte IT wieder hergestellt ist. Wie war das noch mal mit der Forderung auf einen 100% 24/7-Betrieb?

Beispiel Windows Upgrades 11 und Server 2025

Motivation und Ausgangslage

Wie eingangs schon erwähnt, bin ich groß darin, Fehler bei anderen zu sehen und den Finger in die Wunde zu legen. Wie sieht es da im eigenen Netz aus? Ich habe die Vorträge beim NRW IT-Sicherheitstag im Dezember 2024 dazu genutzt, mich selbst noch einmal zu fragen, ob in meinem kleinen IT-Netz alles im grünen Bereich ist und tatsächlich noch ein paar Punkte gefunden, an denen ich nachschärfen konnte. Das betraf zunächst die Firewall, die Kontrolle der Backups und die Aktualisierung der Software. Vieles ist dank monatlicher oder jährlicher Abos seit langem auf einem top-aktuellen Stand, aber man findet immer noch eine Stelle, wo man erneut nachlegen kann. So habe ich alle Windows 10 Rechner auf Windows 11 aktualisiert, übrigens auch die, die laut Microsoft angeblich dazu nicht in der Lage sind (siehe nächstes Kapitel). Von klassischen Office-Versionen habe ich mich schon vor zwei Jahren verabschiedet und setze auf M365. Hier schätze ich nicht nur die Aktualität, sondern auch neue Features, die mir ein sicheres und effektives Arbeiten an jedem Punkt der Welt ermöglichen.

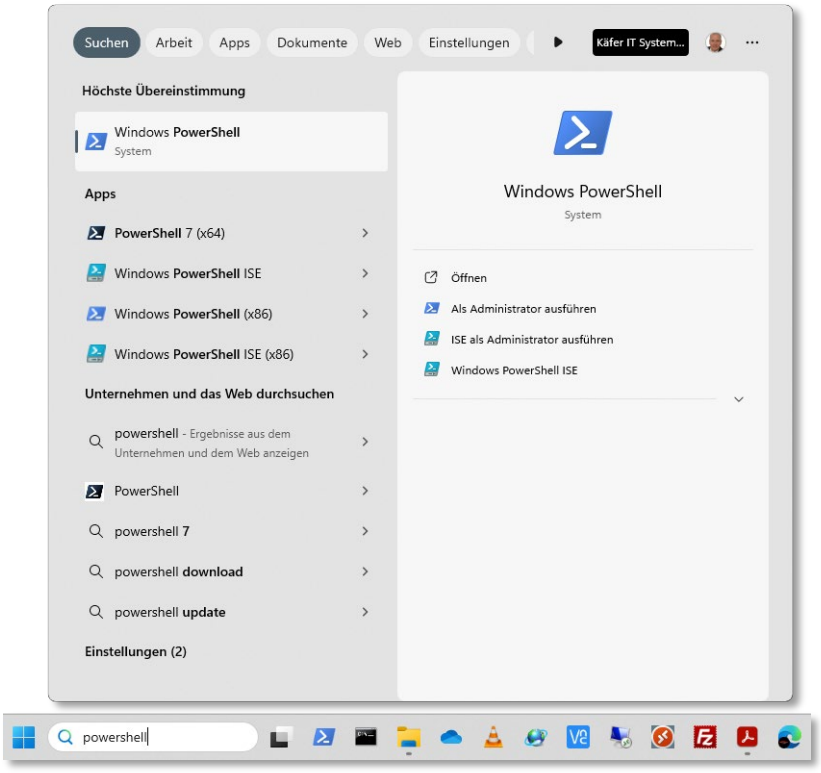
Beim Backup vertraue ich auf mehrere Stufen aus Tape- und Festplattenbackup. Damit habe ich nicht nur mehrere top-aktuelle Sicherungen meist vom Vortag, sondern auch länger aufbewahrte Versionen, die im Tresor und fernab von jedem Hackerzugriff liegen. Das eine oder andere landet zudem noch in der Cloud und damit ist genug getan. Nicht schaden kann es aber, wenn man ab und zu auch kontrolliert, dass alle Backups noch laufen. Der Schreck war schon da, als ich feststellen musste, dass ein paar der Instanzen seit Wochen nicht mehr gestartet worden waren. Von vier möglichen Versionen hatte ich plötzlich nur noch zwei, die funktioniert hatten: Problem erkannt, Problem gebannt und als regelmäßige Aufgabe in den Terminkalender eingetragen.

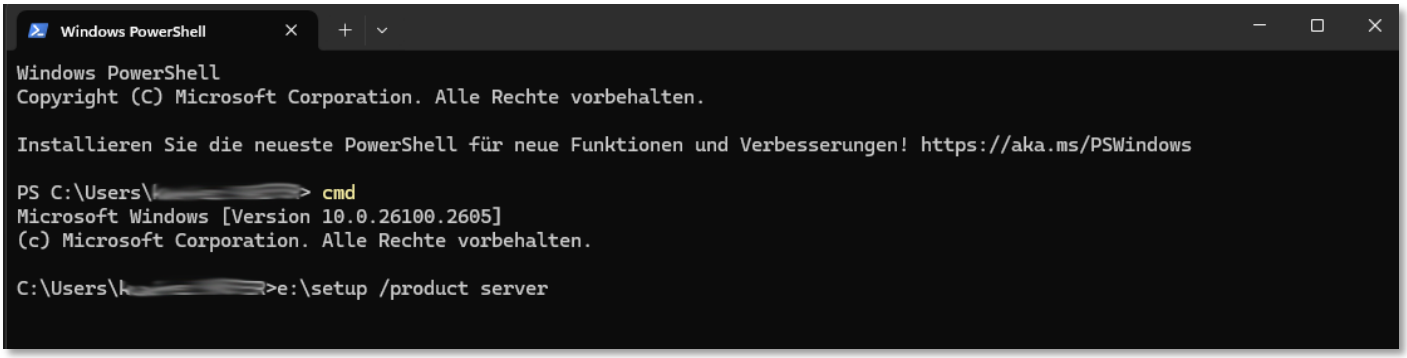
Windows 11 Upgrade

Der Support für Windows 10 endet am 14. Oktober 2025. Aber warum bis dahin warten? Windows 11 läuft prima und eine einheitliche Landschaft ist auch administrativ als One-Man-Show ein Vorteil. Doch Microsoft lässt das über das Windows-Update angebotene und kostenfreie Upgrade von Windows 10 auf 11 nur auf Rechnern zu, die alle Voraussetzungen seitens Microsoft erfüllen. Manchmal reicht schon, dass der Prozessor formal nicht unterstützt wird. Deswegen jetzt teure Hardware wegschmeißen? Bitte nicht. Mit folgendem Trick (auf eigene Gefahr) klappt es auch bei über 12 Jahre alter Apple Mac Hardware, die nach wie vor brav ihren Dienst als Spezialsystem versieht oder einem kleinen NUC, der angeblich zu schwach wäre.

Die Lösung:

1. Handelt es sich um ein System, das man im Zweifelsfall nicht einfach so beim Upgrade-Versuch verlieren will, dann macht man davon ein Backup.
2. Anschließend lädt man sich eine Windows 11 ISO-Datei als Download auf den Rechner und schafft etwas Platz auf der C-Partition.
3. Ein Doppelklick auf die ISO-Datei mountet sie als ein virtuelles Laufwerk mit einem Laufwerksbuchstaben (z.B. E:) und man kann die Setup-Exe per Doppelklick im Explorer öffnen.
4. Bricht der Updateprozess mit einer Fehlermeldung ab, dass das System nicht geeignet ist, kann man auf eigene Gefahr Punkt 5) versuchen.
5. Man öffnet über „Ausführen“ eine PowerShell mit Administratorrechten und gibt darin den Befehl „cmd“ ein.
6. Anschließend wechselt man auf das Laufwerk, in dem die ISO-Datei gemountet wurde und ruft das Programm „setup“ mit dem Parameter „/product server“ auf. Die ganze Zeile bei Laufwerk E: lautet also „e:\Setup /product server“. Wichtig ist das Leerzeichen zwischen „product“ und „server“.
7. Anschließend wird ein ganz normales Windows 11 (kein Server) installiert.





Windows Server 2025

Im Netzwerk setzte ich bisher einen Windows 2019 Server als Domänencontroller und Fileserver ein. Früher wurde die Hardware als einer von zwei ESX-Hosts für diverse virtualisierte Systeme eingesetzt. Da hatte ich noch mehrere Mitarbeiter und wir haben verschiedenste Server selbst gehostet. Das ist heute nicht mehr nötig und vieles liegt als Service in der Cloud. An und für sich ist so ein Windows-Server für eine Handvoll Rechner dann auch vollkommen überdimensioniert, aber wenn man sich davon nicht trennen will, bleibt einem hier nichts anderes übrig, als die Software aktuell zu halten. Jetzt hätte ich zunächst auf Windows 2022 upgraden können, aber seit November 2024 gibt es schon die 2025er Version, die wohl weitestgehend mit Windows 11 übereinstimmt. Zudem soll laut Microsoft bei diesem Betriebssystem die Anzahl der Neustarts nach dem Patchen reduziert werden[9]. Da seit Windows 2012 R2 auch InPlace-Upgrades über mehrere Betriebssystemversionen möglich sind, war für mich schnell klar, dass wir „Nägel mit Köpfen“ machen und direkt auf 2025 aktualisieren. Was sonst noch neu ist, findet man u.a. auf der Seite MSxfaq.de[10].

Vorarbeiten

Der Verlust der Konfiguration des Servers incl. AD wäre zu verschmerzen, aber trotzdem ärgerlich. Daher entschied ich mich, eine nicht mehr benötigte 1TB- SATA-Platte als Backup-Medium einzusetzen und darauf die Windows Server-Sicherung einzurichten. Den Erfolg der Sicherung habe ich am nächsten Tag kontrolliert und hatte somit schon einmal ein Backup für alle Fälle (das ich dann tatsächlich gebraucht habe).

Des Weiteren habe ich recherchiert, wie das Upgrade vonstattengeht und welche Lizenzen ich dazu benötige. Eine sehr gute und funktionierende Anleitung fand ich bei „Frankys Web“[11]. Auf der Suche nach günstigen legalen Software-Lizenzen stieß ich auf das Angebot von Lizenzstar[12]. Sehr positiv fand ich hier, dass man meine Nachfragen zur Lizenzierung auch am Sonntagnachmittag mit sehr kurzer Reaktionszeit vollumfänglich und kompetent beantwortet hat. Damit war klar, dass ich die Software auch von dort beziehen würde. Zunächst besorgte ich mir jedoch eine 180 Tage Evaluation-Version von der offiziellen Microsoft-Seite[13] als ISO-Download. Das hat den Vorteil, dass man das System zunächst ein halbes Jahr kostenfrei und unverbindlich testen kann und die Lizenzierung später nur ein Mausklick ist.

Nach dem Download der ISO-Datei reicht ein Doppelklick darauf und die Datei wird als ISO-Image mit einem Laufwerkbuchstaben gemountet.

---

[9] Quelle Microsoft: https://learn.microsoft.com/de-de/windows-server/get-started/whats-new-windows-server-2025
[10] Quelle: MSxFAQ: https://www.msxfaq.de/windows/windows_server_2025.htm
[11] Quelle Frankys Web: https://www.frankysweb.de/windows-server-2025-domain-controller-inplace-upgrade/
[12] Quelle Lizenzstar: https://lizenzstar.de/
[13] Quelle Microsoft: https://www.microsoft.com/de-de/evalcenter/evaluate-windows-server-2025

Die Vorbereitung der Gesamtstruktur und der Domain ist dann in zwei einfachen Schritten erledigt (Annahme: Die ISO-Datei wurde als Laufwerk E: gemountet):

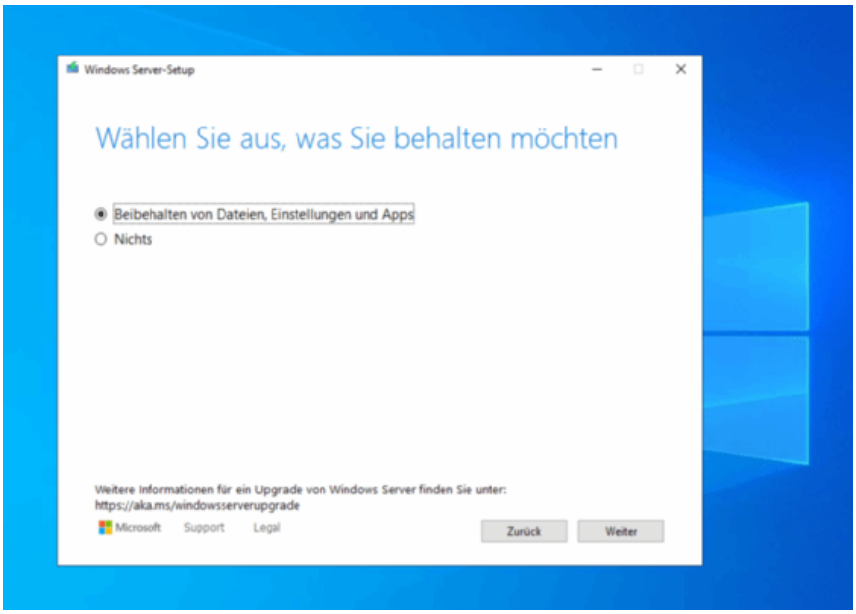
CMD als Administrator aufrufen und dann nacheinander folgende Befehle eintippen
E:
cd support/adprep
adprep /forestprep

Läuft das sauber durch, anschließend noch den folgenden Befehl eingeben:
adprep /domainprep

In der ausführlichen Anleitung von Frankys Web wird darauf hingewiesen, dass sinnvollerweise jede Drittsoftware für die Installation deaktiviert wird. Das schließt auch den Virenscanner ein.

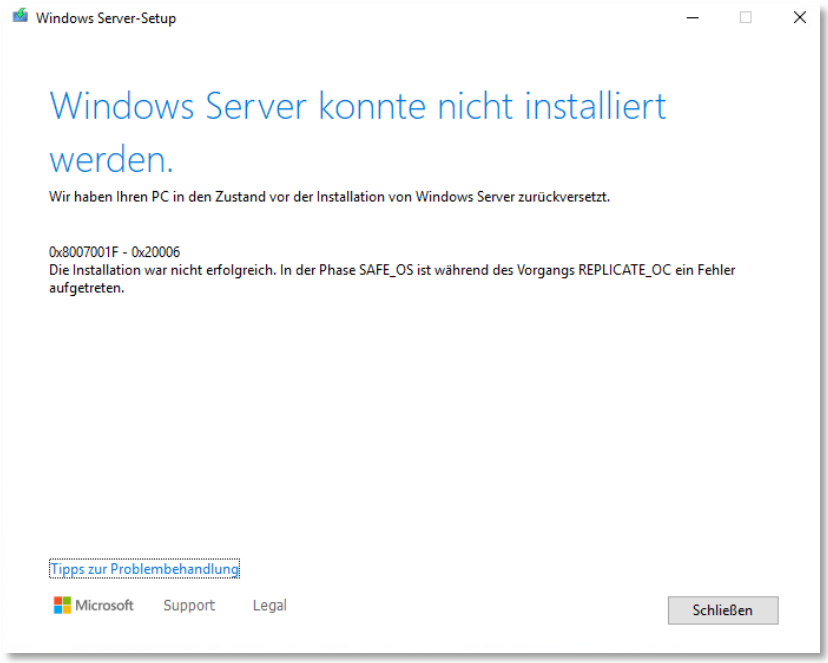
Probleme

Jetzt reicht eigentlich ein Doppelklick auf setup.exe und es geht los.



Die Überraschung war groß, als in einem der folgenden Dialoge die Option „Beibehalten von Dateien, Einstellungen und Apps“ nicht anwählbar war. Einen neuen Server aufsetzen wollte ich ja gerade nicht.

Ein zweites Problem ergab sich (nach der Lösung von Aufgabe Nr. 1 s.u.) dadurch, dass das Upgrade im ersten Versuch nicht erfolgreich durchlief.



Das Zurücksetzen hat aber nicht richtig funktioniert und ich lief ständig in Fehler. Bei einem Neustart hing der PC in einer Bootschleife, um mir dann in der dritten Runde die Reparaturoptionen anzuzeigen. Jetzt war es gut, ein Backup zu haben und ich stellte den Server kurzerhand von der letzten Serversicherung wieder her.

Lösungen

Das erste Problem lässt sich durch einen Trick lösen, der wohl schon bei Server 2012 geholfen hat:

Die Lösung dazu fand ich in Andys Blog[14]:

Man kopiert den Inhalt z.B. der “Windows Server 20xx Eval.iso” auf ein lokales Laufwerk (z.B. nach “E:\W20xx”), erstellt zusätzlich einen leeren Ordner (z.B. “E:\Mount”) und führt der Reihe nach die folgenden Befehle aus:

```
dism /mount-wim /wimfile:E:\W20xx\sources\install.wim /mountdir:E:\Mount /index:2
dism /image:E:\Mount /get-currentedition
dism /image:E:\Mount /get-targeteditions
dism /image:E:\Mount /set-edition:ServerStandard
dism /unmount-wim /mountdir:E:\Mount /commit
```

Danach konnte ich nun tatsächlich die Option „Beibehalten von Dateien, Einstellungen und Apps“ auswählen.

Bevor ich jedoch einen erneuten Versuch gewagt habe, habe ich tatsächlich konsequent alle Drittsoftware und zudem temporär auch die Windows-Firewall deaktiviert. Ob das tatsächlich die Ursache war, ist nicht sicher, aber es gilt wie so oft die zweite Abhilfeempfehlung der IT: Versuche es einfach noch einmal (Nr.1 ist ein Neustart).

Ergebnis

Die Installation lief geschmeidig durch und nach etwa zwei Stunden konnte ich wieder auf den Server mit allem Drum und Dran zugreifen. Jetzt den Virenschutz, Ransomware-Schutz und die Firewall aktivieren, Dritt-Software reaktivieren und den Server noch einmal neu starten. Die Tests mit der Backup-Software verliefen ebenfalls positiv und so habe ich den Server schon einen Tag später mit einem offiziellen Key von Lizenzstar vom Eval-Modus in den lizenzierten Modus angehoben. Fertig.

Fazit

Und die Moral von der Geschichte? Upgrades kosten Zeit, Geld und manchmal Nerven. Sie nicht durchzuführen und zu verschleppen, kostet noch mehr Zeit, Geld und sicher Nerven.

Jetzt haben Sie die Wahl: Lieber Updates machen oder sich hacken lassen?

Übrigens: Wenn Sie sich für die zweite Option entscheiden und in Kürze Opfer einer Cyber-Attacke geworden sind, rufen Sie gerne an. Mein Geld verdiene ich primär damit, Incident-Response und Forensik zu machen und weniger, kostenlose Warnungen wie diesen Aufsatz zu publizieren. Vielleicht war er aber ja nur kostenlos jedoch nicht umsonst.

Aber jetzt ernsthaft: Vielleicht kontaktieren Sie mich tatsächlich, bevor etwas Schlimmes passiert, für eine Systemberatung. Das ist viel entspannter als mich nachher bei einem Incident Response dazuzuholen.

---

[14] Quelle Andys Blog: https://www.andysblog.de/windows-server-inplace-upgrade-mit-evaluierungs-installations-medium