Sieben Security-Tipps für Windows

Printout von blog.jakobs.systems

Tomas Jakobs

29 Dezember 2024

Inhaltsverzeichnis

Schnell umsetzbare und technisch wenig aufwändige Tipps zum Absichern von Windows-Netzwerken:

1. Software Restrictions aktivieren

Die seit XP in jedem Windows enthaltenen Software Restrictions[1] aktivieren und per Gruppenrichtlinien im AD ausrollen. Wo alleinstehende Rechner außerhalb des AD im gleichen Segment stehen, müssen SRPs manuell in den lokalen Sicherheitsrichtlinien aktiviert werden.[2] Auch wenn von Microsoft offiziell abgekündigt und bei Windows 11 aus Vorsatz oder Dummheit einen (leicht behebbaren) Bug eingebaut,[3] stellen SRP weiterhin die sicherste und am weitesten funktionierende Implementierung eines App-Whitelisting dar.

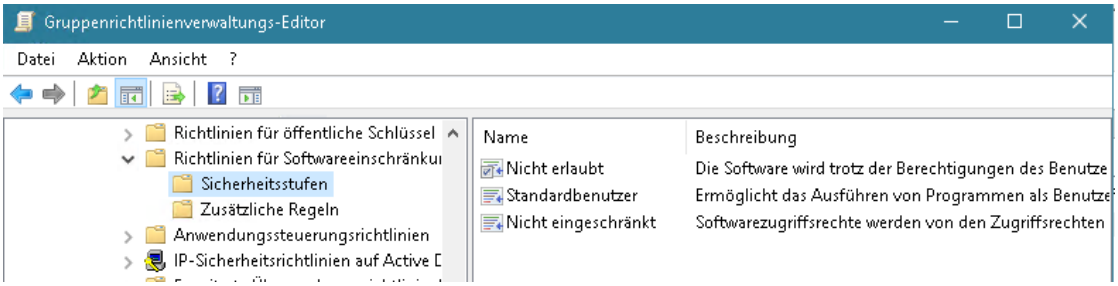

Abbildung 1: Aktivierung der SRP in den GPOs einer AD

2. Windows-Rechner offline betreiben

Das komplette AD ist mit seine Hosts per Firewall-Regeln am Internet-Gateway offline zu halten. Internetzugriff erfolgt ausschließlich über einen Squid[4] Web-Proxy. Die Proxy-Informationen werden ebenfalls per GPO nur dem Firefox-Webbrowser mitgeteilt und für Benutzer nicht veränderbar gemacht.

---

[1] https://learn.microsoft.com/de-de/windows-server/identity/software-restriction-policies/administer-software-restriction-policies

[2] https://schneegans.de/windows/safer/

[3] https://blog.jakobs.systems/micro/20230223-vorsatz-srp-in-win11/

[4] https://www.squid-cache.org/

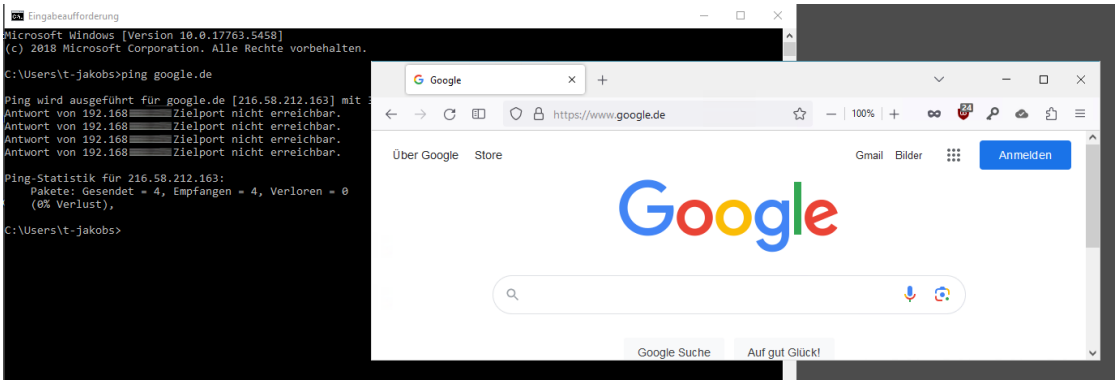

Abbildung 2: Windows bleibt offline, nur Firefox darf raus

Auf keinen Fall die Proxy-Daten in den Windows-Systemeinstellungen hinterlegen. Benutzern via GPO die Rechte entziehen, diese im System setzen zu können.

Windows-Updates gelangen weiterhin via WSUS[5] auf die Systeme, wo als einzige Ausnahme ebenfalls der Proxy Server hinterlegt ist.

3. Externe Zugänge kontrollieren

Wird das interne AD offline gesetzt, muss der Zugang von außen anders gewährleistet und kontrolliert werden. Sowohl für eigene Mitarbeiter, als auch für externe Dienstleister. Die üblichen Verdächtigen Teamviewer & Co scheiden kategorisch aus. Diese Zugänge sind schlicht nicht kontrollierbar, benötigen dauerhafte Internetverbindungen und Client-Software Installationen, die pro Gerät zusätzlich zu warten sind.

Ein handelsüblicher Webbrowser stellt die am besten verfügbare und flexibelste Möglichkeit eines Remote-Zugriffes dar. Wie das mit dem RDP2HTTP Gateway Apache Guacamole realisiert werden kann, das habe ich bereits hier vorgestellt.[6]

[5] https://de.wikipedia.org/wiki/Windows_Server_Update_Services

[6] https://blog.jakobs.systems/blog/20231010-supplychain-management/

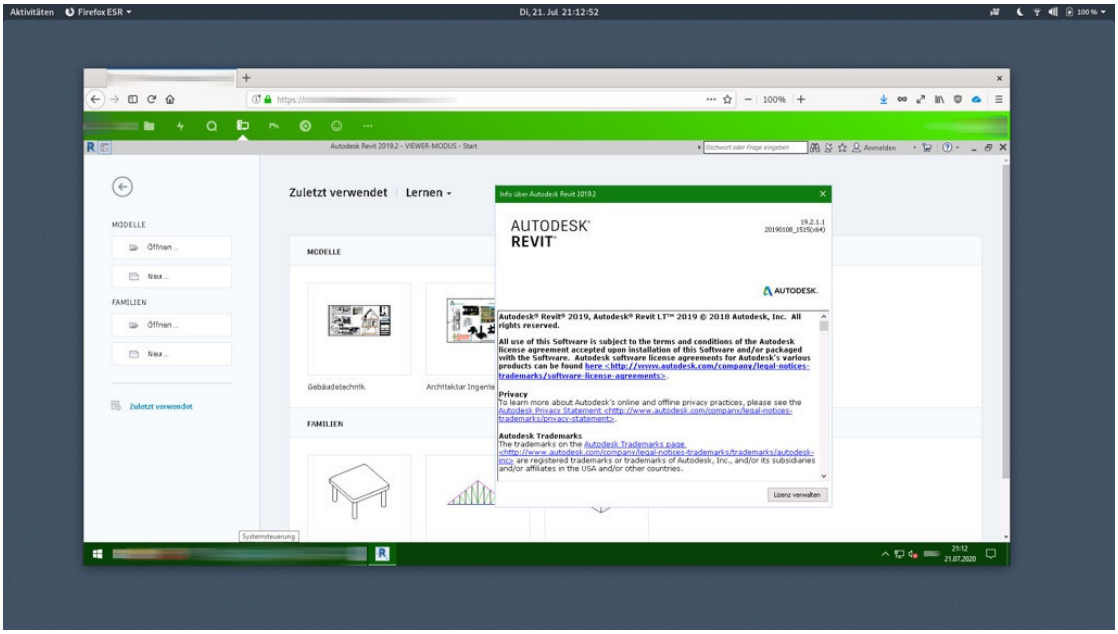

Abbildung 3: Zugriff aus der Ferne auf den Firmen-Arbeitsplatz

Als problematisch erweisen sich die “Wanderer zwischen den Welten”. Das sind Benutzer mit Ihren mobilen Endgeräten, die “dual homed” zwischen Firmennetzwerk und anderen, potentiell unsicheren Netzen wandern. Das betrifft auch alle mit externer VPN-Einwahl. Wie in meiner Homeoffice-Serie hingewiesen, bilden diese die schwächste Stelle in einem Sicherheitskonzept.[7]

Diese sind alle aus dem AD zu entfernen und Arbeitsplätze per Terminalserver zur Verfügung zu stellen. Das stößt erfahrungsgemäß auf Widerstand bei den Betroffenen, bringt aber auch enorme Vorteile: Ein handelsüblicher Webbrowser reicht zur Verbindung in die Firma aus, die Wahl des Endgerätes wird beliebig.

Diese ersten drei Maßnahmen reduzieren in Ihrer Kombination das Risiko erheblich bei einem überschaubaren Aufwand. Natürlich sollte ein ADs auch im internen Netz mit vLANs von Produktionsanlagen, Webcams, Druckern und einem WLAN isoliert werden. Your milage may vary.

[7] https://blog.jakobs.systems/blog/homeoffice/

4. Mail-Gateways nutzen, Exchange abschalten

Den eigenen SMTP-Mailserver nur durch einen Mail-Gateway wie beispielsweise von Proxmox[8] mit dem Internet kommunizieren lassen. Erneut eine einfache, schnell umsetzbare Maßnahme. Idealerweise in Kombination mit einer GoBD[9] konformen Email-Archivierung, wenn noch nicht erfolgt.

Wer für seinen lokal betriebenen Microsoft Exchange Server noch immer keinen Ersatz gefunden hat, sollte langsam aktiv werden. Den Bock zum Gärtner machen leider viele, die den vermeintlich einfachen Microsoft-Way in die Cloud folgen. Außer erhebliche Preisaufschläge, unbekannte Kostenrisiken in der Zukunft, Kontrollverlust bei deutlich erhöhten Administrationskosten ist nichts gewonnen. Mir persönlich sind mittelständische Unternehmen bekannt, die allein für den Support neue Stellen ausschreiben mussten, wo zuvor ohne Microsoft 365 keine notwendig waren.

Wer es bequem und komfortabel will, findet zahlreiche linuxbasierte Workgrouplösungen wie z.B. Grammunio[10]. Prinzipiell lässt sich jedes Debian als Mailserver nehmen. Das für Outlook benötigte ActiveSync wird mit SoGo[11] erreicht inkl. öffentliche Ordner und einem übersichtlichen Web-Interface.

[8] https://proxmox.com/de/proxmox-mail-gateway/uebersicht

[9] https://de.wikipedia.org/w/index.php?title=GoBD

[10] https://grommunio.com/

[11] https://sogo.nu/

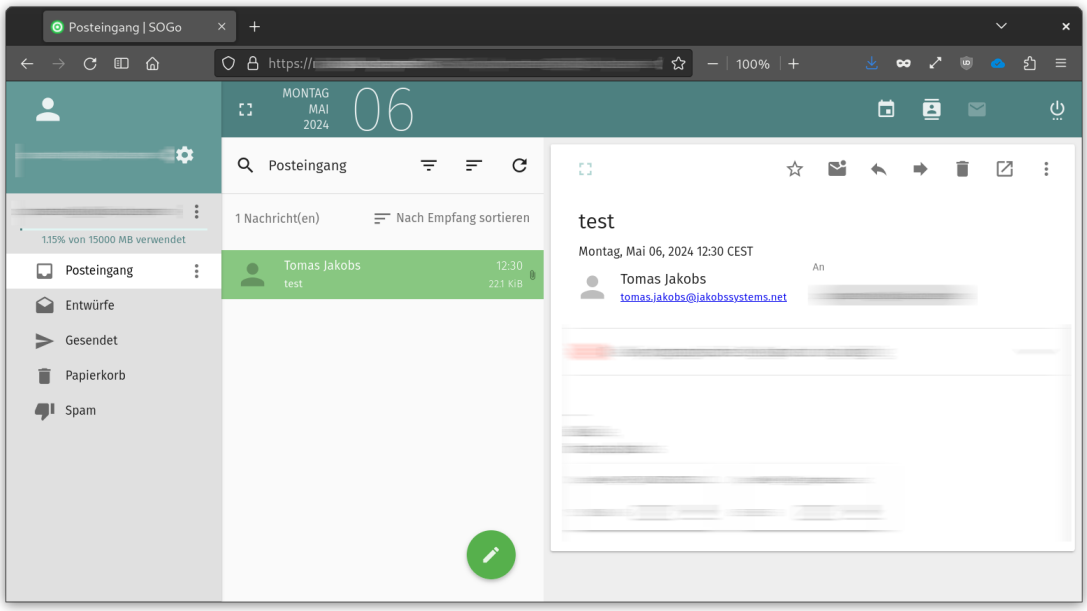

Abbildung 4: SoGo Webmailer mit 2FA und allen Funktionen

5. Email-Anlagen filtern

Am Mailserver oder Gateway das Filtern von unerwünschten Anhängen aktivieren. Idealerweise erfolgt das mit einer Allow-List, die alles Unbekannte und insbesondere .doc, .xls sowie alle ausführbaren Dateien pauschal entfernt oder mit einer informativen Textdatei ersetzt.

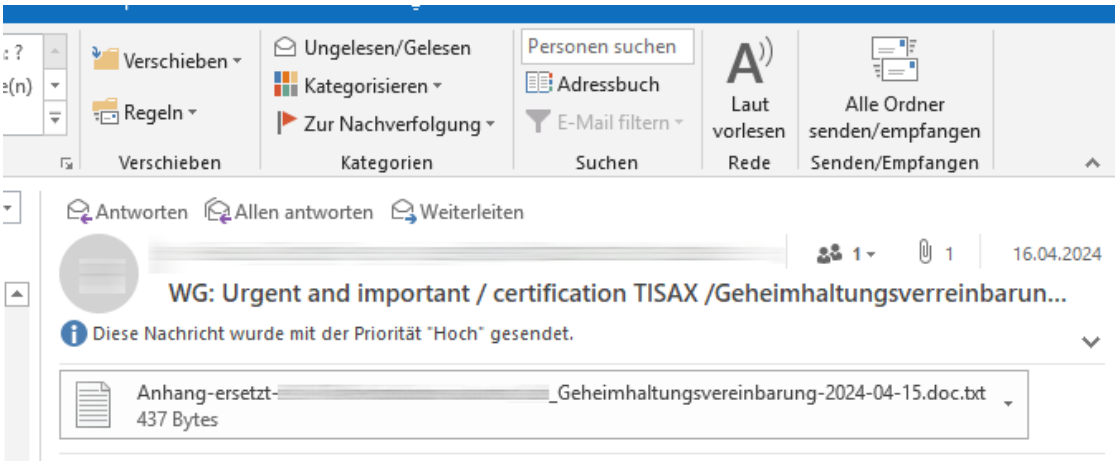

Abbildung 5: Unerwünschte Mail-Anlagen, hier eine .doc Datei durch Textdatei ersetzt

Eine schnelle und minimal-invasive Maßnahme, die erwartungsgemäß zu Widerständen auf Anwenderseite führt. Excel- und Word-Dokumente können nicht mehr wie gewohnt per Mail ausgetauscht werden. Bessere und modernere Arten wie zum Beispiel der Austausch über die eigene Nextcloud[12] oder die Nutzung der in jeder Nextcloud enthaltenen Collabora Online-Office-Lösung[13] werden nicht sofort als Verbesserung wahrgenommen.

Für mich ist die Handhabung von E-Mail Anlagen Heuristik für den Zustand der Digitalisierung. Jede manuell verschickte Excel-Liste ist Indiz für kaputte Prozesse und/oder miserable Warenwirtschaft, die das nicht von selbst hinbekommt.

6. Kein 3rd-Party SSO

Keine externen SSO[14] Anbieter verwenden und Anmeldedaten nicht an Dritte weitergeben. Die Schutzziele[15] der Informationssicherheit “Vertraulichkeit” und “Integrität” können in Folge nicht mehr gewährleistet werden. Jeder, der sein Outlook hybrid mit ModernAuth[16] betreibt, gewährt Microsoft einen nicht mehr transparent nachvollziehbaren, uneingeschränkten Zugriff auf seine Daten.

Die Erfahrung im Operations zeigt: Wer nicht in der Lage ist, seine Zugangsdaten und 2FA in einem Passwortmanager zu verwalten, wird mit SSO ebenfalls Probleme haben. Das Versprechen, mit einem einfach zu merkenden Passwort sich überall authentifizieren zu können hinkt ohnehin, da die besten Kennwörter genau jene sind, die sich nicht einfach merken lassen. Zudem kommen Mitarbeiter gerade im Umgang mit externen B2B-Portalen und Plattformen nicht umhin, am Ende des Tages doch wieder einen Passwortmanager anzuwerfen.

Wer auf die Bequemlichkeit von SSO nicht verzichten mag, findet mit privacyIDEA[17] oder Keycloak[18] zwei bewährte und selbst zu betreibende Alternativen unter Beibehaltung der vollen digitalen Souveränität.

---

[12] https://nextcloud.com/

[13] https://nextcloud.com/blog/how-to-install-collabora-online-in-nextcloud-hub/

[14] https://de.wikipedia.org/wiki/Single_Sign-on

[15] https://de.wikipedia.org/wiki/Informationssicherheit

[16] https://learn.microsoft.com/en-us/microsoft-365/enterprise/hybrid-modern-auth-overview

[17] https://privacyidea.org/

[18] https://keycloak.org/

7. Keine Daily-Driver-Admins

Windows-Admins[19] und das Management stellen die größten Sicherheits-Risiken dar. Opportun sind höhere Rechte oder Ausnahmen von Regeln selbst schnell vergeben und anschließend noch schneller vergessen. Das sind die Sargnägel von jedem Versuch, eine gelebte Sicherheitskultur einzuführen.

Admins und Management haben auf der gleichen Ebene zu arbeiten, wie alle anderen auch. Administrative Eingriffe erfolgen standardisiert nur bei Bedarf, idealerweise auf strikt überwachten Jumphosts mit extra Admin-Konten. Das Vier-Augen-Prinzip bewährt sich nicht nur bei der gegenseitigen Kontrolle und bildet ein Sicherheitsfeature, sondern erhöht nebenbei auch die Transparenz in Admin-Teams.

Ohnehin zählen manuelle Eingriffe direkt auf den Systemen eher zur seltenen Ausnahme. LAPS[20], Git-Ops Workflows[21], Ansible[22], meinetwegen die selbst-geschriebene Bash- und PowerShell-Sammlung, müssen Standard für wiederkehrende Aufgaben sein. Der nachfolgende Screenshot zeigt, wie ein Admin in IDE oder Texteditor nur noch mit Git-Repos arbeitet, ohne mit den zu verwaltenden Servern verbunden zu sein:

[19] https://blog.jakobs.systems/micro/20230913-lockout-admins/

[20] https://learn.microsoft.com/de-de/windows-server/identity/laps/laps-overview

[21] https://www.redhat.com/de/topics/devops/what-is-gitops

[22] https://www.ansible.com/

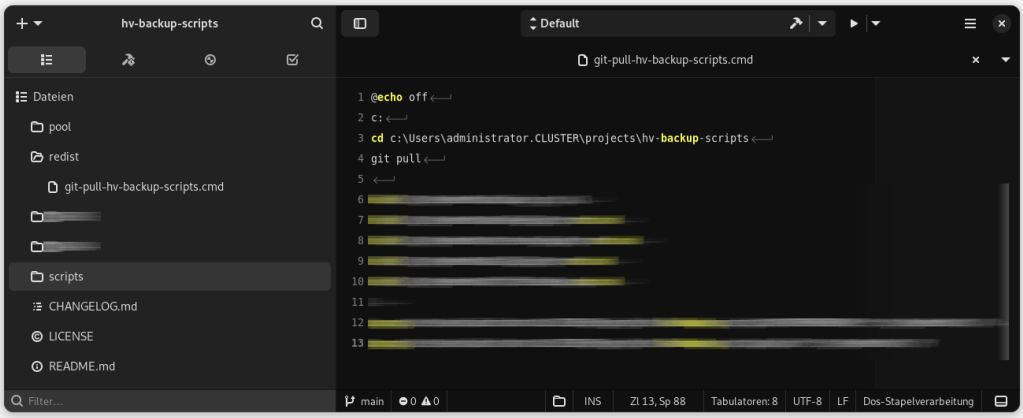

Abbildung 6: Serververwaltung mit Git-Ops Workflows und Skripten

Fazit:

Mögen diese sieben Tipps helfen, damit niemand im Märchenland umher irren muss.[23] Aber Obacht! Es sind meist nicht die technischen Dinge, die der Resillienz und Sicherheit entgegen stehen. Das Mindset und der Wille sind entscheidend. Auf die Versprechen von Microsoft war hingegen noch nie Verlass.[24] Alles bereits vor Jahren gesehen und gehört, Geschichte wiederholt sich aber nicht.[25]

Mein letzter Tipp: Einmal Last Week Tonight mit John Oliver zur Causa Boeing anschauen.[26] Die kulturellen Ähnlichkeiten zu Microsoft sind kaum zu übersehen.

In diesem Sinne,
Euer Tomas Jakobs

[23] https://heise.de/news/jakobssystems-9708160.html

[24] https://heise.de/news/jakobssystems-9708577.html

[25] https://blog.jakobs.systems/micro/20240404-history-repeating/

[26] https://youtube.com/watch?v=Q8oCilY4szc