Fefes Blog - Windows Security

Originalartikel

Backup

<html> [l] Ich ringe immer mit mir, ob ich Tipps verbreiten soll, wie man Dinge sicherer konfiguriert. Insbesondere wenn es sich um proprietäre Software wie Windows handelt. Auf der einen Seite will ich nicht nur schreiben, wie kaputt alles ist. Auf der anderen Seite will ich aber auch nicht dafür sorgen, dass Leute länger bei Windows bleiben, weil sie dank irgendwelcher Konfigurationsratschläge den Eindruck haben, sie könnten das schon irgendwie absichern. Zu guter Letzt bin ich Code Auditor, nicht Admin. Was man da alles konfigurieren kann ist nicht mein Spezialgebiet. Am Ende verbreite ich noch Unfug? Daher haben meine Zero-Trust-Folien am Ende eine eher allgemeine Vision. Allerdings kam ein Leserbrief mit konkreten Ratschlägen rein, den ich jetzt mal veröffentlichen möchte. Nehmt das aber bitte nicht als abzuarbeitendes Howto sondern als Grundlage für eigene Recherchen. Ziel der Übung sollte sein, dass ihr ein bisschen mehr verstanden habt, wie die Dinge funktionieren. <blockquote> zu deiner Zero Trust Präsi möchte ich mal etwas zur Windows Security einwerfen. Sorry, ist etwas länglich geworden. Wir sind IT Dienstleister und übernehmen in der Regel den Service einer bestehenden IT Landschaft die entweder vorher durch den Kunden oder durch einen anderen Dienstleister betreut wurde. KMU 1 bis 500 MA.Dahin zu gehen und den Kunden Windows und Outlook wegzunehmen wird in der Regel nicht gelingen. Wenn es möglich ist einen neuen Server auf Linux hoch zu ziehen könnte man das vorschlagen und umsetzen, da hört es aber dann auch schon auf. Der Satz „Das geht, weil Sie Outlook und Office benutzen“ stimmt leider in den meisten Fällen, obwohl das nicht so sein müsste.MS liefert schon seit Windows 2000 allerhand Techniken mit die genau das alles verhindern. Wir haben aber noch nicht einen Kunden bekommen bei dem irgendwas davon aktiv war und holen das alles schleunigst nach. Das schlimmste was uns als Dienstleister passieren kann, ist ein Ransomwarebefall eines Kunden bei dem wir die Schuld tragen, weil deren Systeme nicht sicher sind, obwohl man es *ohne* Anschaffung zusätzlicher Software hätte besser machen können. Der Kunde verlässt sich darauf dass wir ihm eine sichere Arbeitsumgebung geben. Es ist ein Unding, dass ein aktueller Windows Server bei einer frischen Active Directory Installation immer noch fast die gleichen Sicherheitsdefaults verwendet wie es in 2000 eingeführt wurde und so kommt es, dass von all dem was nun kommt in freier Wildbahn oft nichts zu sehen ist. 1: Software Restriction Policies (SRP), ja ich weiß ist deprecated, läuft aber selbst auf Win 11 noch. MS wollte das durch Applocker ersetzen. Ist aber auch deprecated. MS will das durch Defender Application Control ersetzen, geht aber nur per XML oder und nur in Enterprise oder so. Wir bleiben bisher bei SRP, weil das keine Enterprise Lizenzen braucht und seit Win 2000 unverändert läuft. Muss man halt nach jedem größerem Update testen ob es noch geht. </blockquote>Anmerkung von mir: Die ct hatte dazu mal ein Tool veröffentlicht, da könnt ihr damit mal herumspielen.<blockquote> Was tut es? Windows führt nur noch EXE, CMD/BAT, PS1, sonstwas aus Pfaden aus die der Admin per GPO festgelegt hat. Outlook kopiert den Anhang aus der Mail in ein Temp Verzeichnis und will es dort starten. Das darf es dann nicht mehr. Admins installieren nach c:\program files\. Das ist erlaubt. Ein User darf da nicht schreiben.MS torpediert es aber selbst mit Programmen die sich unter AppData\Local installieren. Teams z.B. und andere Hersteller sind da auch keine Vorbilder. Muss man sehr enge Ausnahmen setzen und das Risiko in kauf nehmen. 2: Makros. Ja, der gelbe Balken bringt nix. Per GPO hart ganz abschalten. Brauchen ohnehin die wenigsten Anwender. Die die es

brauchen, kann man geziehlt auf die Dokumente einschränken für die es gehen soll. Was machen die Malware Makros? VBS oder Powershell Script ausführen und Payload nachladen und starten. Geht eigentlich durch SRP schon nicht mehr, aber es soll ja Bugs geben die vielleicht um SRP drum rum kommen. </blockquote>GPO ist ein Group Policy Object, oder in deutschen Versionen: Gruppenrichtlinien.<blockquote> 3: Beschafft sich lokale Admin-Rechte und übernimmt den Domain Controller.Wenn 1 und 2 versagt hat kommen wir dahin. Nächste Verteidigungslinie ist Lateral Movement zu verhindern. Es gibt genug GPOs zum härten der Systeme, aber man klemmt halt damit alten Legacy ab, was ich aus technischen Sicht eigentlich ganz gut finde. NTLM Auth weg, Credential Caching für Admins und generell Server abschalten, Debugging Rechte global abschalten und nur im Einzelfall erlauben. LAPS benutzen, auch für Server. Das macht es Mimikatz schon ganz schön schwer an verwertbare Daten zu kommen. </blockquote>In meinen Folien hatte ich gesagt, dass Lateral Movement nicht Teil des Threat Models ist. Ich bin mir unsicher, inwieweit man das verallgemeinern kann. Ich unterhalte mich zu Ransomware mit Kumpels, die weiter oben auf der Eskalationsskala sitzen, die sehen dann praktisch ausschließlich Fälle, bei denen der AD übernommen werden konnte. Ich habe leider keine Zahlen, wie hoch der Prozentsatz der Ransomware-Angriffe ist, die man verhindern könnte, wenn man Lateral Movement unterbindet. ALLERDINGS: Wenn man durch andere Maßnahmen dafür sorgt, dass der Sprung zum Domain Admin nicht geht, dann wird die Verhinderung von Lateral Movement plötzlich eine wichtige Maßnahme. Genau das spricht der Leserbrief hier an.<blockquote> Mit ESAE hat MS schon lang ein Konzept die Admin Ebenen voneinander zu trennen. Man muss auch nicht zwingend mehrere Domänen betreiben um den wichtigsten Teil davon umzusetzen.Bei uns darf ein Domain Admin nicht mal PCs in Domänen aufnehmen. Niemals sollte sich ein Domain Admin an einem Client anmelden und das lässt sich auch per GPO verhindern.Der darf auch nur an Domain Controller, die CA und ähnliche Systeme. Ein Server Admin darf da nicht hin und der darf auch nicht an Clients. Ja, der Domain Admin hat dann halt 4 User Accounts. User, Client Admin, Server Admin, Domain Admin. Natürlich mit Grundverschiedenen Passwörtern. Kommt man mit klar. </blockquote>Ich hab das in einem Nebensatz irgendwo erwähnt, dass man die Admin-Accounts aufteilen soll, und dass der Domain Admin nicht an die Datenbanken können soll. Der Leser hier hat völlig Recht, das kann und sollte man noch mehr auftrennen. Dann hat man tatsächlich etwas getan, um im Threat Model ein Bedrohungsrisiko zu senken.<blockquote> Selbst ein Keylogger auf dem Client bekommt dann höchstens den Admin für die Clients, aber kann immer noch nicht auf Server oder gar Domain Controller. 4. Benutz Smart Cards für die Admins und lass nur Anmeldungen per Smart Card zu. In dem Fall kann ein Keylogger auf dem PC auch das Kennwort nicht einfach mal mitlesen.USB Smart Cards sind nicht teuer. Die Menge an Admins überschaubar.Für RDP gibt es dann noch den Restricted Admin Mode mit entsprechenden Komforteinbußen.In Enterprise Editionen noch Credential Guard, usw. </blockquote>Dazu sei angemerkt, dass auch mit Smart Cards im Hintergrund immer noch Kerberos läuft mit Kerberos-Tickets, die abgreifbar sind. Aber die laufen wenigstens nach einer Weile aus.<blockquote> 5. Exchange kann Split Permissions. Nutzt das. Es entfernt die Berechtigungen dass der Exchange Server Domain Admin Rechte hat. HAFNIUM war damit nur halb so schlimm.Server müssen auch nicht überall ins Internet dürfen. Verhindert dass Malware auf euren Servern ganz bequem per HTTPS ihren Payload laden können. Erweitert das noch mit VLANs und Firewalls. Kein Anwender muss auf die ESXi Infrastruktur, einen Switch oder das BMC vom Server. Die müssen auch auf die wenigsten Ports für die Anwendungsserver. Da reichen oft ACLs auf dem Core Switch um zumindest bei Line Speed zu bleiben. </blockquote>Für die BMC und Hypervisoren würde ich dringend zu physisch getrennter Verkabelung raten, statt zu irgendwelchen Software-Geschichten.<blockquote> Backupserver aus der AD nehmen. Per Firewall/ACL einschränken, dass der an die Server darf, aber die Server nicht zum

Backupsserver. </blockquote>Das ist ein guter Ratschlag!<blockquote> All diese Dinge die ich beschrieben habe gehen mit Bordmitteln. Da ist nicht ein Anti-Virus, SIEM oder sonst eine 3rd Party Lösung beteiligt.Wir setzen das meiste davon bei Firmen ein die keine 10 Mitarbeiter haben. Das kann man mit Routine an einem Tag umsetzen. (Den Windows Teil zumindest) Testet das selbst mit Mimikatz, Bloodhound und was auch immer. Hackt euch selbst und danach oder wenn ihr das generell nicht könnt, holt euch noch einen Pen Tester um die offensichlichen Lücken weg zu machen. Am Rande: Domain Joined Device Public Key Authentication muss man nicht einschalten. Das ist per Default an. Man muss es aber erzwingen wenn man das Fallback nicht haben will. Ist fast das gleiche, aber doch nicht ganz und geht erst mit Server 2016. Am weiteren Rande: Patchmanagement. Es wäre schön, wenn MS nicht Patches raus bringen würden die großflächig zu Boot Loops auf Domain Controllern, Druckproblemen oder 802.1X/802.11X Problemen führen würden. Dann hätte man auch mit Auto-Updates weniger schmerzen. So muss man eigentlich schon zwangsweise ein paar Tage warten, wenn man nicht vor einem Totalausfall am nächsten Tag stehen möchte. Beides verfahren sind somit schlecht. Ich gehe nicht davon aus das danach das System unhackbar sicher ist. Wir sprechen hier immer noch von Software und von Microsoft, aber zumindest hat man etwas in die richtige Richtung getan und die offenlichtlichen Scheunentore geschlossen. Wer nun mit dem erhöhten Supportaufwand argumentiert, dem sei gesagt dass er bei uns gesunken ist, weil die Anwender eben nicht mehr alles ausführen können was bei 3 nicht auf den Bäumen ist und die Computer dadurch so bleiben wie der Admin es sich mal vorgestellt hat.Entwicklungsabteilungen können zusätzlich Nicht-Domain Computer oder VMs bekommen um ihre systemnahe Arbeit durchzuführen. </blockquote>Nur ein Nachsatz noch von mir: Der Feind ist Komplexität. Es ist zwar schön, dass man bei Microsoft eine Menge konfigurieren kann, so dass es weniger schlimm ist, aber am Ende des Tages überblickt niemand mehr den ganzen Softwarehaufen, und alle sind nur an der Oberfläche am Herumkratzen. Das betrifft glücklicherweise auch die meisten Angreifer. Wirklich sicher fühlen würde ich mich da nicht. Und wenn man erstmal diese Art von Knowhow aufgebaut hat, dann wird man wahrscheinlich nie wieder von Windows wegmigrieren wollen. Aus meiner Sicht ist der Vorteil von Linux und co, dass es da keine natürliche Schranke gibt, wie viel Verständnis man von dem Gesamtsystem aufbauen kann. </html>