Beratung · boddenberg.de

Beratung Windows-Firewall: einschalten ohne Ausfall

Unabhängige Begleitung vom ersten Lagecheck bis zur scharf geschalteten, zentral gesteuerten Windows-Firewall, per GPO oder Intune

Bei dir ist die Windows-Firewall aus, zumindest im Domänenprofil, und eigentlich weiß jeder, dass das so nicht bleiben kann? Dann geht es dir wie erstaunlich vielen Organisationen. Meistens fehlt nicht der Wille, sondern die Antwort auf eine einzige Frage: **Was geht kaputt, wenn wir sie einschalten?** Genau diese Frage beantworte ich mit dir, bevor irgendetwas scharf geschaltet wird.

Ich berate seit rund 30 Jahren in Microsoft-Umgebungen, in Mittelstand, Kliniken und Verwaltungen. Für dieses Thema habe ich ein eigenes Werkzeug gebaut: Der Windows Firewall Diagnostiker zeigt je Anwendung, welche Ports offen sind, welche Regel sie freigibt und was beim Einschalten blockiert würde. Das spart dir Beratertage, und wir reden über Befunde statt über Vermutungen.

Die Beratung auf einen Blick	
Für wen	Organisationen mit abgeschalteter oder unklar konfigurierter Windows-Firewall auf Servern und Clients, Systemhäuser mit entsprechenden Kundenprojekten
Themen	Lagecheck, Lernmodus, Regelwerk, GPO-Design, Scharfschalten in Ringen, Ausnahmenprozess, Umzug der Firewall-Regeln nach Intune
Vorgehen	Drei Bausteine: Lagecheck, Einführung, Betrieb und Intune; einzeln oder zusammen buchbar
Werkzeug	Windows Firewall Diagnostiker, kostenlos und ausschließlich lesend, bis du etwas ausdrücklich freigibst
Ort	Remote per Teams oder vor Ort, Sitz in Dortmund
Konditionen	Auf Anfrage, gern als Festpreis für klar umrissene Bausteine

Warum das Einschalten so oft scheitert

Technisch ist eine Firewall in zehn Sekunden eingeschaltet. Dass es trotzdem jahrelang niemand macht, hat Gründe, die du wahrscheinlich kennst:

- **Niemand weiß, was gebraucht wird.** Fachanwendungen, Agenten für Fernwartung, Monitoring und Backup, Druck, Scanner, Medizintechnik oder Maschinensteuerung: Dokumentiert ist davon wenig.
- **Die Steuerung ist undurchsichtig.** Eine alte „Aus“-GPO, ein paar lokale Regeln, vielleicht schon Intune dazu. Wer gewinnt, weiß keiner so genau.
- **Es gibt keinen Rückweg.** Wer einschaltet und Pech hat, steht am Montagmorgen mit der halben Klinik oder der Produktion am Telefon.
- **Keine Zeit.** Das Thema ist wichtig, aber nie dringend. Bis der Pentest-Bericht oder der Vorfall kommt.

> **Warum es trotzdem sein muss**
>
> Ohne Host-Firewall kann jede Maschine jede andere über SMB, RPC, WinRM und RDP erreichen. Genau diese Wege nutzen Angreifer nach dem ersten Treffer, um sich auszubreiten. Eine eingeschaltete Windows-Firewall ist eine der wirksamsten Maßnahmen gegen seitliche Bewegung im Netz, und sie ist auf jeder Windows-Maschine schon vorhanden.

Drei Bausteine, ein Ziel: Firewall an, Betrieb läuft

Du kannst an jeder Stelle einsteigen, je nachdem, wo du gerade stehst.



Die drei Bausteine der Beratung

Baustein 1: Lagecheck

Wir starten mit einer ehrlichen Bestandsaufnahme. Mit dem Windows Firewall Diagnostiker scannen wir deine Server, auf Wunsch auch eine Auswahl an Clients, per Kommandozeile auf eine Freigabe. Daraus entsteht ein Sammelbericht. Parallel schauen wir uns an, welche GPOs und Intune-Richtlinien die Firewall heute steuern und wo sie sich widersprechen.

- Lücken je Rolle und Anwendung: Was würde beim Einschalten blockiert, und warum?
- Analyse der Steuerung: „Aus“-GPOs, Rangfolge, Erzwungen, Regelzusammenführung, Mischbetrieb mit Intune
- Einschätzung, wo es wehtun wird, und wo nicht
- Lagebericht mit Einführungsplan, den du auch an Geschäftsführung, Datenschutz oder Dienstleister weitergeben kannst

Baustein 2: Einführung

Aus dem Plan wird Wirklichkeit, und zwar so, dass in keiner Phase ein großer Knall droht:

- **Lernphase:** Eine Lern-GPO für eine Pilotgruppe schaltet die Firewall an, lässt eingehend aber weiter alles zu und protokolliert. Es wird nichts blockiert, aber alles sichtbar.
- **Regelwerk:** Wir werten aus, was tatsächlich gebraucht wird, klären Unklares mit Fachabteilungen und Herstellern und testen mit Testregeln, die sich selbst wieder abräumen.
- **GPO-Design:** Eine Basis-GPO für alle, Rollen-GPOs für Datenbank-, Datei-, Druck- oder Terminalserver, sauber benannt und dokumentiert.

- **Scharfschalten in Ringen:** erst der Pilot, dann OU für OU, kritische Systeme zuletzt. Die alte „Aus“-GPO bleibt bis zum Schluss stehen, der Rückweg ist in jeder Phase derselbe.

> **Typischer Fund: die Regel im falschen Profil**
>
> Ein typisches Bild: Die Firewall ist auf allen Servern per GPO im Domänenprofil abgeschaltet, in den Profilen Privat und Öffentlich aber an. Viele Installer haben brav eine Freigabe angelegt, nur eben für „Privat“. Entfernt man die „Aus“-GPO einfach, sind genau diese Dienste beim nächsten Richtlinienabgleich weg. Der Lagecheck findet sie vorher, und das Einschalten wird zum Nicht-Ereignis.

Baustein 3: Betrieb und Intune

Eine Firewall-Einführung ist erst fertig, wenn das Regelwerk auch nach der nächsten Softwareinstallation noch stimmt.

- **Ausnahmenprozess:** Wer beantragt eine Freigabe, wer genehmigt, wann läuft sie ab? Dazu ein Ausnahmenregister, das Audits standhält.
- **Umzug nach Intune:** Du willst weg von der GPO? Wir überführen das Regelwerk in Intune-Richtlinien, prüfen die Grenzen und vermeiden die Falle, dass beides gleichzeitig wirkt.
- **Drift erkennen:** Regelmäßige Scans zeigen, wo neue Ports aufgetaucht sind oder Regeln verschwunden sind.
- **Workshop für dein Team:** Wie die Windows-Firewall wirklich entscheidet, wie das Werkzeug funktioniert und wie man neue Anwendungen sauber freigibt.

Typische Anlässe

Anlass	Was wir tun
Firewall per GPO aus	Lagecheck, Lern-GPO mit höherer Rangfolge für eine Pilotgruppe, Einführung in Ringen
Pentest- oder Audit-Befund	Befund einordnen, schnell wirksame Maßnahmen für Clients, Plan für die Server, Nachweis über das Ausnahmenregister
Nach einem Vorfall	Seitliche Bewegung erschweren: Client-zu-Client-Verkehr sperren, Verwaltungszugriffe auf das Admin-Netz beschränken
Hersteller sagt „Firewall aus“	Tatsächlichen Bedarf der Anwendung messen und gezielt freigeben, statt die ganze Maschine aufzumachen
Umzug nach Intune	Bestand aus GPOs aufnehmen, bereinigen, nach Intune überführen, Mischbetrieb vermeiden
Umgebung übernommen	Bestandsaufnahme und Dokumentation eines Regelwerks, das jemand anderes gebaut hat

Passt gut, wenn …

Passt gut	Passt eher nicht
Du betreibst eine Active-Directory- oder Intune-Umgebung mit Windows-Servern und -Clients	Du suchst Beratung zu einer Perimeter-Firewall eines bestimmten Herstellers

Passt gut	Passt eher nicht
Du willst Befunde mit Belegen statt Meinungen	Du willst die Firewall „bis Freitag“ ohne Lernphase scharf haben
Du willst das Regelwerk danach selbst pflegen können	Du suchst einen 24/7-Betriebsdienstleister
Du bist Systemhaus und willst Unterstützung bei Kundenprojekten	

Für Systemhäuser

Viele Projekte laufen gemeinsam mit Systemhäusern. Du bleibst Ansprechpartner deines Kunden, ich steige dort ein, wo es knifflig wird: GPO-Rangfolge, Regelzusammenführung, Lern-GPO, Intune-Migration. Den Windows Firewall Diagnostiker kann dein Team kostenlos selbst einsetzen, auch beim nächsten Kunden.

Häufige Fragen zur Beratung

Wie lange dauert der Lagecheck?

Die Scans selbst dauern je Maschine Sekunden bis wenige Minuten. Mit Auswertung der GPOs, Besprechung und Lagebericht sind es meist wenige Tage, abhängig von der Zahl der Rollen und Standorte.

Ändert der Lagecheck etwas an meinen Servern?

Nein. Der Windows Firewall Diagnostiker arbeitet im Lagecheck ausschließlich lesend. Geändert wird erst in der Einführung, und dann nur nach ausdrücklicher Freigabe, mit Sicherung und Rückweg.

Wie lange muss die Lernphase laufen?

So lange, bis keine neuen Zugriffe mehr auftauchen. Mit Monatsabschluss, Backup-Läufen und Patchday sind das in der Praxis rund vier Wochen.

Geht das auch komplett remote?

Ja, die meisten Projekte laufen remote per Teams. Für Workshops komme ich auf Wunsch auch vorbei.

Was ist, wenn ein Hersteller auf „Firewall aus“ besteht?

Dann messen wir, was die Anwendung tatsächlich braucht, und geben genau das frei, eingeschränkt auf die nötigen Quellen. Mit diesen Daten lässt sich mit Herstellern meist gut reden.

Müssen wir dafür auf Intune umsteigen?

Nein. Die Einführung funktioniert genauso mit Gruppenrichtlinien. Wer ohnehin nach Intune will, kann das Regelwerk aber gleich dort aufbauen.

Was kostet die Beratung?

Das hängt von Größe und Vorhaben ab. Nach einem kurzen Gespräch bekommst du ein konkretes Angebot, gern als Festpreis für den Lagecheck.

Lass uns reden

Schreib mir über die Kontaktseite oder stell deine Frage direkt über „Frag Uli“ am Ende der Seite. Erzähl mir kurz, wie viele Server und Clients du hast, wer die Firewall heute steuert und wo es zwickt, dann schlage ich dir einen Termin vor.

Werkzeug

Der Windows Firewall Diagnostiker im Detail: Anwendungskarte, Lernmodus, Abgleich.

Zum Windows Firewall Diagnostiker

Download

Kostenlos, eine EXE, keine Installation.

Jetzt herunterladen

Kontakt

Termin für ein erstes Gespräch vereinbaren.

Zur Kontaktseite