



HORNETSECURITY
BY proofpoint.



DAS MSP PLAYBOOK

FÜR INTELLIGENTERES STATT HÄRTERES ARBEITEN

KAPITEL 1: EINFÜHRUNG IN DIE STEIGERUNG DER EFFIZIENZ VON MSPs

Dieses Buch zeigt Ihnen praxisnahe Strategien, mit denen Sie verschiedene Geschäftsbereiche effizienter gestalten und in einer sich schnell wandelnden Branche wettbewerbsfähig bleiben. Durch den Einsatz der vorgestellten Empfehlungen und Werkzeuge, gewinnen Sie Einblicke in die Arbeitsweisen besonders erfolgreicher MSPs, steigern Ihre Profitabilität und bleiben den Anforderungen immer einen Schritt voraus.

MSPs stehen vor beispiellosen Herausforderungen und Chancen. Wir zeigen, wie erfolgreiche MSPs Automatisierung eingesetzt haben, um Abläufe zu optimieren und Kosten zu senken, ohne die so wichtige Kundenbeziehung zu gefährden. Dieses eBook führt Sie durch die wesentlichen Strategien, um in diesem dynamischen Umfeld erfolgreich zu sein.

WIE WIR AN DIESEN PUNKT GEKOMMEN SIND

Das Geschäftsmodell, das wir heute Managed Service Provider (MSP) nennen, entstand in einer Zeit, als Infrastruktur lokal betrieben wurde und sich im Besitz des Kunden befand. Server waren allgegenwärtig, Computer standen meist fest auf dem Schreibtisch und waren per Ethernet-Kabel verbunden, und am Wochenende wurde im Büro kaum gearbeitet. Der MSP strebte danach, die ausgelagerte IT-Abteilung des Unternehmens zu werden und brachte Kostenvorteile, indem er seine Zeit auf mehrere Kunden verteilte. Das MSP-Personal selbst war hoch spezialisiert auf Infrastruktur, Bereitstellung und Fehlerbehebung. Die meisten Arbeiten wurden manuell und vor Ort ausgeführt. Die Werkzeuge zur Fehlerbehebung beschränkten sich häufig auf Hilfsmittel wie TechNet, Wireshark und Kabeltester. Viel Pizza und koffeinhaltige Getränke gehörten bei Server-Upgrades, langen Troubleshooting-Sitzungen mit Microsoft am Telefon und bei Treffen von Benutzergruppen ganz selbstverständlich dazu.

DANN KAM DIE CLOUD.

Mit der Cloud änderte sich das erforderliche Kompetenzprofil. Statt sich auf Serverinstallation und -konnektivität zu konzentrieren, mussten MSPs lernen, Anwendungen aus der Ferne zu verwalten. Die steigende Nachfrage nach Dienstleistungen und nach einer größeren Bandbreite an Services zwang MSPs dazu, mehr Personal einzustellen und es auf mehr Kunden zu verteilen, um trotz sinkender Margen profitabel zu bleiben. Hoch rentable Infrastrukturprojekte wurden zunehmend durch Software-Abonnements mit geringer Marge und dauerhaftem Verwaltungsaufwand ersetzt.

DANN KAMEN DIE CYBERKRIMINELLEN.

Die Cloud erhöhte die Angriffsfläche für Unternehmen und machte es für Cyberkriminelle einfacher, an sensible Daten zu gelangen. In der Folge entwickelten Angreifer immer raffiniertere Werkzeuge und Methoden – darunter die Bedrohungen, die uns heute in Form von Ransomware und Phishing begegnen. Zwar existierten Hacking und Malware schon lange zuvor, doch mit dem Aufkommen moderner Ransomware ab etwa 2013 nahmen die Auswirkungen auf den Geschäftsbetrieb deutlich zu. Dann kamen die Cyberversicherungsbranche und Compliance-Vorgaben ins Spiel.

Als Lösegelder bezahlt wurden, explodierte die Cyberkriminalität, und es entstand eine immer komplexere Landschaft branchenspezifischer Cyber-Compliance-Anforderungen. MSPs fanden sich an vorderster Front der Verteidigung wieder, oft ohne das nötige Skillset oder ein passendes Preismodell, um den Bedarf ihrer Kunden abzudecken. Deshalb mussten sie sich schnell neu ausrichten, um diesen neuen Anforderungen gerecht zu werden. Die meisten investierten massiv in immer mehr Softwaretools, um Kompetenzlücken zu schließen und repetitive Aufgaben zu automatisieren. Heute geben MSPs in der Regel 20 % oder mehr ihres Umsatzes für Software-Toolsets aus, was sich zu einer durch Ineffizienz getriebenen Krise entwickelt hat.



DANN KAM KI UND SIE IST VERMUTLICH DIE GRÖSSTE DISRUPTIVE VERÄNDERUNG, DIE UNSERE BRANCHE SEIT JAHRZEHNEN ERLEBT HAT.

Als ChatGPT vor einigen Jahren im Bewusstsein der breiten Öffentlichkeit ankam, erahnten nur wenige das enorme Ausmaß, in dem generative KI die Gesellschaft, Fehlinformationen, den Klimawandel und natürlich die Geschäftswelt beeinflussen würde. MSPs müssen sich erneut weiterbilden und umstellen, diesmal jedoch in einem Umfeld, das sich rasend schnell verändert. Haben Sie letzte Woche noch etwas über Copilot-Agenten gelernt? Das ist schon wieder veraltet, denn heute dreht sich alles um OpenClaw-Agenten. MSPs spielen eine wichtige Rolle dabei, ihre Kunden bei der Einführung von KI zur Effizienzsteigerung zu begleiten und gleichzeitig sicherzustellen, dass die Sicherheit nicht beeinträchtigt wird. Es gibt aber auch die andere Seite: den internen Einsatz von KI, um einen MSP effizienter zu machen. Wir werden uns beide Bereiche ansehen und zeigen, wie MSPs sie bewältigen können, ohne die KI-Landschaft aus dem Blick zu verlieren.

ALS MSP EFFIZIENT UND PROFITABEL WACHSEN

All diese Veränderungen in der Branche passieren schnell, doch das Geschäftsmodell hat sich nur langsam angepasst. Viele MSPs haben Schwierigkeiten, ihre Profitabilität in einer Branche zu erhalten, die früher für hohe Margen und gut bezahlte Arbeitsplätze bekannt war. Die gute Nachricht ist: Unternehmen wissen, dass sie MSPs brauchen, und MSPs wissen, dass sie sich modernisieren müssen, um erfolgreich und profitabel zu bleiben.

In diesem eBook betrachten wir mehrere zentrale Bereiche des MSP-Betriebs, zeigen Effizienzpotenziale auf und schlagen Wege vor, sie zu nutzen. Ein besonderer Schwerpunkt liegt dabei auf Microsoft 365, generativer KI und Agenten sowie Cybersecurity. Wir konzentrieren uns bewusst nicht auf einzelne technische Detailfragen oder finanzielle Kennzahlen. Stattdessen erhalten Sie einen praxisnahen Überblick darüber, wie moderne MSPs effizient arbeiten, nachhaltiges Wachstum schaffen und den steigenden Anforderungen des Marktes erfolgreich begegnen. Das Ergebnis: Sie verstehen besser, wie die Branche weiterhin gute Arbeitsplätze schaffen, notwendige Services liefern und technische Herausforderungen wie Cybersecurity und Compliance beherrschbar machen kann. MSPs sind heute ein entscheidender Erfolgsfaktor für Unternehmen weltweit. Wenn MSPs effizient und zukunftssicher aufgestellt sind, profitieren Kunden, Mitarbeitende und die gesamte Branche gleichermaßen. Sind Sie bereit, Ihr MSP-Geschäft zu transformieren und ein neues Maß an Effizienz zu erreichen? Dann beginnen wir mit der ersten Aufgabe, der ein MSP bei einem neuen Kunden begegnet: dem Onboarding.



 AUTOMATE  STANDARDIZE  GOVERN



365 MULTI-TENANT MANAGER FOR MSPS

KOSTENLOS
TESTEN



KAPITEL 2: ONBOARDING

Das Onboarding wird oft als Kostenfaktor und Belastung für personelle Ressourcen betrachtet. Dieses Kapitel soll diese Sichtweise ändern, indem es die Vorteile eines gut umgesetzten Onboarding-Prozesses darlegt und Tipps zur Steigerung der Effizienz gibt.

ZWEI SICHTWEISEN AUF DAS ONBOARDING

Zu verstehen, wie ein Kunde die Arbeit eines MSP wahrnimmt, ist nicht immer einfach. Kunden, die vielleicht nicht sehr technisch versiert sind, achten stärker auf das Erlebnis der Zusammenarbeit, während MSPs meist technisch und ergebnisorientiert sind. Gerade deshalb ist der Onboarding-Prozess eine entscheidende Gelegenheit, neue Kunden zu beeindrucken und zu begeistern.

Was beeindruckt den Kunden? Was begeistert den Kunden?

BEEINDRUCKEN	BEGEISTERN
Professionalität	Individuelle Betreuung
Effizienz	Reaktionsschnelligkeit
Expertise	Freundlichkeit
Zuverlässigkeit	Liebe zum Detail

Auf welche Ergebnisse konzentriert sich der MSP?

ONBOARDING-ERGEBNISSE	
Endgeräte an die Management-Lösung anbinden	Migration zu Microsoft 365-Lösungen
Endgeräte sichern	Ausfallzeiten minimieren
Anwendungen bereitstellen	MSP-Toolset bereitstellen
Compliance-Anforderungen konfigurieren	Schnelle Fertigstellung

ONBOARDING AUS SICHT DES KUNDEN

Immer häufiger sind es die Soft Skills, anhand derer Ihr Kunde Sie bewertet. Zu Beginn wird er wahrscheinlich annehmen, dass sich gute technische Kompetenz überall finden lässt. Ausschlaggebend war daher Ihr Verkaufsprozess, der ihn dazu bewogen hat, sich für Sie zu entscheiden: Ihr Elevator Pitch, Ihre Website und die Vermittlung Ihres Alleinstellungsmerkmals. Wird das positive Gefühl im Onboarding beeinträchtigt, kann dies die Kundenbeziehung bereits in der Anfangsphase negativ beeinflussen. Der Kunde sollte daher vom ersten Tag an ein überzeugendes Erlebnis haben.

Übertragen wir die beiden obigen Übersichten in die Praxis, sollten sich MSP-Mitarbeiter auf Folgendes konzentrieren.

1 PROFESSIONALITÄT:

- » **Klare Kommunikation:** Kommunizieren Sie während des gesamten Onboardings klar und konsistent. Erklären Sie jeden Schritt in verständlicher Sprache und legen Sie klare Erwartungen fest. Gute Kommunikation hilft Kunden dabei, ruhig und geduldig zu bleiben, weil sie mögliche Herausforderungen einordnet.
- » **Dokumentation:** Stellen Sie eine verständliche Dokumentation für alle Prozesse und Abläufe bereit. So versteht der Kunde, was geschieht, und hat eine Referenz für die Veränderungen in seinem Umfeld.
- » **Auftreten:** Alle Interaktionen, ob vor Ort oder virtuell, müssen professionell ablaufen. Dazu gehören angemessene Kleidung sowie ein professionelles und zugleich freundliches Auftreten.

2 EFFIZIENZ:

- » **Optimierte Prozesse:** Kunden verstehen vielleicht technische Details nicht, erkennen aber sehr wohl Ineffizienz. Führen Sie einen wiederholbaren Onboarding-Prozess ein und nutzen Sie Erkenntnisse aus jedem neuen Kundenprojekt, um die Erfahrung für den nächsten Kunden zu verbessern.
- » **Automatisierung:** Automatisieren Sie das Onboarding in Intune, um Konfiguration, Compliance, Sicherheitskonfiguration und die Bereitstellung von Anwendungen auf Windows- und anderen Endgeräten zu vereinfachen.
- » **Schnelle Lösung:** Reagieren Sie zügig und effizient auf Probleme oder Rückfragen, um Ausfallzeiten zu minimieren und ein reibungsloses Onboarding sicherzustellen. Vergessen Sie nicht, den Kunden während des gesamten Prozesses auf dem Laufenden zu halten und holen Sie Rückmeldungen des Kunden zum Lösungsprozess ein.

3 EXPERTISE:

- » **Wissensvermittlung:** Bereiten Sie den Kunden mit einem kurzen Termin auf das Onboarding vor und erklären Sie die einzelnen Schritte. Teilen Sie danach Ihr Wissen durch Schulungen und Materialien, damit der Kunde die bereitgestellten Services versteht und nutzen kann.
- » **Problemlösung:** Stellen Sie Ihre Kompetenz unter Beweis, indem Sie technische Probleme, die während des Onboardings auftreten, direkt lösen. Verschieben Sie Anomalien nicht auf später, denn der Kunde wird jedes verbleibende Problem als fehlgeschlagenes oder unvollständiges Onboarding betrachten.
- » **Kundenspezifische Anpassung:** Passen Sie das Onboarding an die konkreten Anforderungen des Kunden an und zeigen Sie so Ihre Fähigkeit für individuelle Lösungen. Schon einfache Dinge wie Logo, Firmenname und Hintergrundbild vermitteln, dass die Lösung speziell für diesen Kunden gedacht ist.

4 ZUVERLÄSSIGKEIT:

- » **Konstante Performance:** Neue Kunden haben möglicherweise schlechte Erfahrungen mit früheren MSPs gemacht. Stellen Sie sicher, dass alle Aufgaben korrekt und termingerecht abgeschlossen werden, um Vertrauen aufzubauen.
- » **Weiterverfolgung:** Nehmen Sie nach Abschluss des Onboardings Kontakt beim Kunden auf, um offene Anliegen zu klären und die Zufriedenheit sicherzustellen. Glaubt der Kunde, dass etwas übersehen wurde, sollte das Problem sofort gelöst werden.
- » **Verlässlicher Support:** Bieten Sie während des Onboardings und darüber hinaus verlässliche Unterstützung, damit sich der Kunde gut betreut und wertgeschätzt fühlt.

Wenn MSPs diese Punkte erfüllen, folgt die Zufriedenheit von selbst. Durch den Fokus auf Professionalität, Effizienz, Expertise und Zuverlässigkeit schaffen MSPs ein positives Onboarding-Erlebnis. Wenn Sie nach dem Eindruck des Kunden fragen, sollten Begriffe wie „freundlich“, „professionell“, „kompetent“ und „fachkundig“ fallen. Dann wissen Sie, dass Sie hervorragende Arbeit zur Festigung der Kundenbeziehung geleistet haben.

Oft sind es die kleinen Dinge. Ich erinnere mich an das Onboarding eines Kunden, der noch einen lokalen Server hatte. Der Geschäftsführer war erstaunt, dass wir kleine Etiketten für jedes Kabel am Server und an der Netzwerkverkabelung druckten. Er sagte, das habe zuvor niemand gemacht. Ich erklärte, dass die Zusatzzeit, die wir heute investieren, in einer späteren Krisensituation sehr viel Zeit sparen kann. Alles zu beschriften und zu dokumentieren, gehört zu einem guten Onboarding.

Nutzen Sie auch die Tatsache, dass Sie wahrscheinlich nicht der erste MSP sind, den dieses Unternehmen im Laufe der Jahre beauftragt hat. Vor Vertragsabschluss und während des Onboardings werden Sie vermutlich einige kritische Anmerkungen über den bisherigen MSP hören. Denn wäre der Kunde mit dessen Leistungen vollständig zufrieden gewesen, hätte er sich nicht für einen Wechsel zu Ihnen entschieden. Nutzen Sie dieses Wissen, um dieselben Fehler nicht zu wiederholen und eine gute Grundlage für die Geschäftsbeziehung zu schaffen.

ONBOARDING AUS SICHT DES MSP

Was ein erfolgreiches Onboarding bedeutet, kann aus Sicht des Kunden und aus Sicht des MSP sehr unterschiedlich sein. Für den Kunden steht meist im Vordergrund, dass die Umstellung reibungslos funktioniert und der laufende Geschäftsbetrieb nicht beeinträchtigt wird. Für den MSP hingegen umfasst ein erfolgreiches Onboarding zusätzlich interne Ziele wie effiziente Ressourcennutzung, standardisierte Abläufe und eine wirtschaftliche Umsetzung. Viele dieser Aufgaben bleiben für den Kunden unsichtbar, sind jedoch entscheidend, um den wahrgenommenen Erfolg überhaupt zu ermöglichen.

Erinnern Sie sich an die oben aufgelisteten MSP-Ziele.

Sie fragen sich vielleicht, warum „schnelle Fertigstellung“ auf der Liste steht. Ein schneller Abschluss sorgt für zufriedene Kunden, da sich der Wechsel zu Ihren Services nicht in die Länge zieht und sein Geschäft nicht unnötig stört. Aus Sicht des MSP bedeutet ein schneller Abschluss, dass nur die wirklich erforderliche Arbeitszeit eines Mitarbeiters aufgewendet wird und so Ressourcen effizient eingesetzt werden.

EFFIZIENZ BEIM ONBOARDING

Der erste Schritt zu mehr Effizienz beim Onboarding neuer Kunden ist ein klarer Prozess zur Informationserfassung. Der MSP muss zum Beispiel bestehende Lizenzen, Admin-Passwörter und die Umstellung auf MFA erfassen sowie die Dokumentationen im eigenen System zusammenführen. Die Erfahrung zeigt, dass viele dieser Informationen weder vom Kunden noch vom vorherigen MSP vollständig bereitgestellt werden. In solchen Fällen benötigen Sie eine bewährte Methode, um die Informationen schnell zusammenzutragen.

Effizienz beim Onboarding wird durch Wiederholbarkeit und Automatisierung erreicht. Beides hilft MSPs dabei, profitabel zu bleiben und Kunden zugleich mit Professionalität und souveränem Auftreten zu überzeugen. In Ihrem Microsoft-Partnerkonto erhalten Sie mit AI Cloud Partner – Partner Launch Benefits (früher Action Pack) oder höheren Plänen Zugriff auf mindestens einen Demo-Tenant. Demo-Tenants eignen sich hervorragend dazu, Ihre Standardeinstellungen vorzubereiten.

Ein Nachteil, wenn Sie Ihre Einstellungen ausschließlich in einer Demo-Umgebung vorbereiten, ist, dass Sie diese Einstellungen nicht in der Praxis testen können. Deshalb kann es sinnvoll sein, den produktiven Tenant Ihres eigenen MSP zunächst als Testumgebung für neue Einstellungen zu verwenden. So kann der MSP das Sicherheitsniveau seines am besten geschützten Tenants selbst erleben und kann dieses Niveau als Goldstandard festlegen. Anschließend sollten die Einstellungen in einer zweiten Testphase bei einer Gruppe von Kunden eingeführt werden, die erfahrungsgemäß

offen für Änderungen sind, bevor der flächendeckende Rollout erfolgt. Mit diesem Vorgehen lassen sich Fehler reduzieren und Marketing und Helpdesk erhalten genügend Zeit, um die Kommunikation vorzubereiten und bestehende Abläufe bei Bedarf anzupassen.

AUFGABEN ABSCHLIESSEN

Um Effizienz im Onboarding zu erreichen, müssen MSPs die folgenden vier Aufgaben erfüllen:

- » Automatisierung des Geräte-Onboardings
- » Automatisierung der Gerätekonfiguration
- » Standardisierung der Portalkonfiguration
- » Standardisierung der Sicherheitskontrollen

Mit Hornetsecuritys speziell für MSPs entwickelten 365 Multi-Tenant Manager lassen sich Ihre Tenants sehr einfach in einem zentralen Verwaltungsportal zusammenführen. Dabei können Sie entweder alle Kunden aus dem Microsoft-Partnerportal übernehmen oder gezielt einzelne Tenants auswählen, wie in Abbildung 1 zu sehen.

Sobald die Tenants erfasst sind, stellt Microsoft mehrere Werkzeuge bereit, die die Einbindung von Geräten vereinfachen und für unterschiedliche Kundenszenarien geeignet sind.

- » Windows Autopilot eignet sich ideal für die Automatisierung der Geräteregistrierung und -konfiguration. Es ermöglicht eine optimierte Microsoft Entra-Anmeldung während der Windows Out-of-Box Experience (OOBE) und unterstützt Zero-Touch-Bereitstellungen neuer Geräte.
- » Bulk Enrollment (Massenregistrierung) eignet sich für bestehende Geräte oder Szenarien, in denen Autopilot nicht anwendbar ist.
- » Die Microsoft Device Management (MDM)-Registrierung mit Intune ermöglicht die automatische Registrierung von Geräten in MDM während des Microsoft Entra-Beitrittsprozesses, sodass die Verwaltung sofort nach dem Beitritt zu Ihrer Organisation möglich ist.

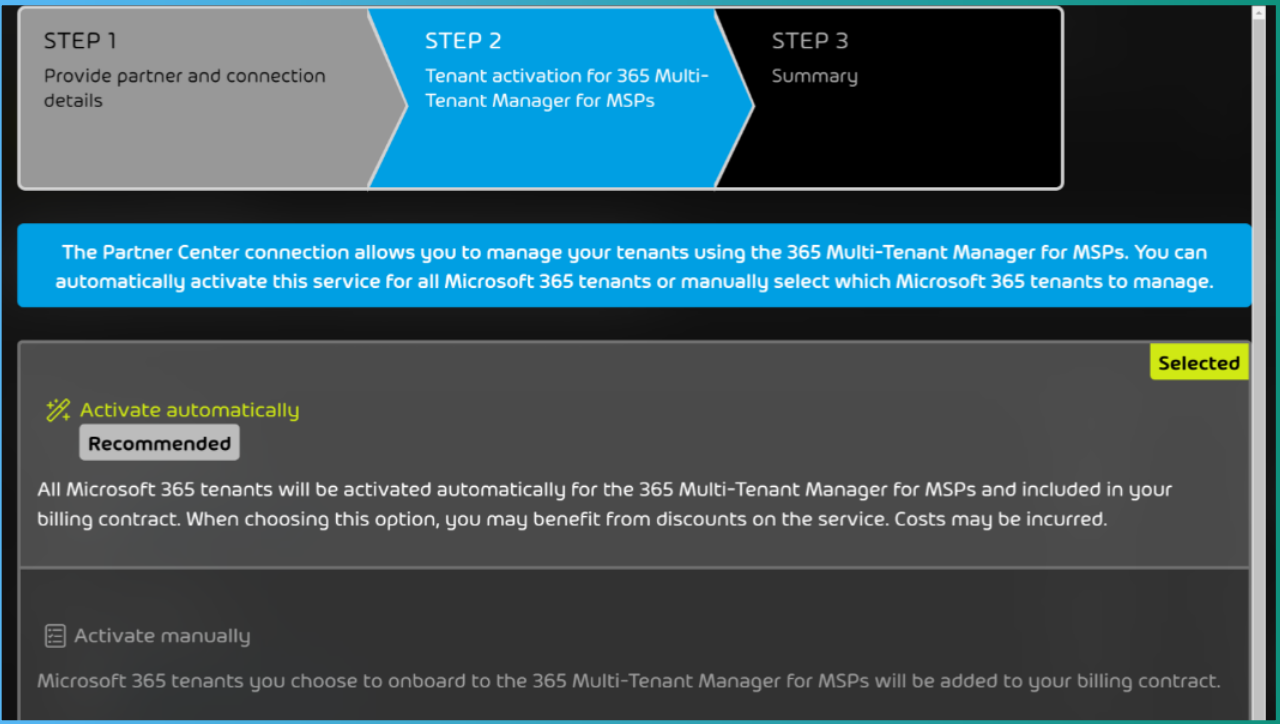


Abbildung 1: Nutzen Sie den Assistenten, um Ihre Tenants schnell in Ihr eigenes Verwaltungsportal zu integrieren

- » Die Self-Service-Registrierung eignet sich gut für BYOD-Szenarien. Benutzer können ihre eigenen Geräte über die Windows-Einstellungen oder über OOBE selbst einbinden, sofern BYOD zugelassen ist.
- » PowerShell und „Scheduled Tasks“ (geplante Aufgaben) können für bereits mit Entra ID verbundene Geräte genutzt werden, die noch in Intune aufgenommen werden müssen. Ein PowerShell-Skript kann deviceenroller.exe mit den passenden Parametern auslösen, oder eine geplante Aufgabe im Systemkontext führt das Registrierungsskript aus.

Nach dem Onboarding mit einer dieser Methoden sind die Geräte bereit für die Konfiguration mit Intune. Intune ist Ihr Werkzeug, um Gerätekonfigurationen und Compliance-Einstellungen zu übertragen. Microsoft stellt Sicherheitsbaselines und Vorlagen zur Verfügung, die Sie bei der Erstellung Ihrer Standards unterstützen.

Ein Schlüssel zur Effizienz ist ein gut dokumentierter Standard mit Checklisten und Standardarbeitsanweisungen (Standard Operating Procedures, SOPs), damit der Prozess bei jedem neuen Kunden von allen Mitarbeitern wiederholbar ist. Ein vollständig automatisiertes Werkzeug dafür ist in Microsoft 365 nicht enthalten. Stattdessen müssen Sie ein Branchenwerkzeug erwerben oder beispielsweise OneNote nutzen.

Der nächste Schritt zu effizientem Onboarding besteht darin, die Portalkonfiguration und Sicherheitskontrollen zu standardisieren. Beides erfolgt bereits während des Onboardings, muss aber anschließend dauerhaft gepflegt werden. Microsoft stellt für die Ersteinrichtung einige Hilfsmittel bereit, darunter Sicherheitsbaselines und das Open-Source-Tool „[M365 Desired State Configuration](#)“. Auch die neuen [Tenant Configuration Management APIs](#), die sich derzeit noch in der Vorschau befinden, kommen dafür grundsätzlich in Frage. Allerdings hat jedes dieser Tools seine Grenzen. Wer die Sicherheitsrichtlinien verwendet, muss Änderungen bei neuen Veröffentlichungen von Microsoft testen und anpassen. Zudem sind die bereitgestellten Baselines in der Regel sehr strikt, sodass eine vollständige Implementierung die tägliche Arbeit vieler Benutzer erschweren kann. Deshalb müssen diese Vorgaben für jeden Kunden individuell getestet werden. Sobald Sie Ihren Standard definiert haben, können Sie mit dem Werkzeug Ihrer Wahl eine standardisierte Zielkonfiguration erstellen. Diese Konfiguration lässt sich dann mit identischen Einstellungen auf weitere Tenants übertragen.

In der Praxis empfinden viele MSPs diese Werkzeuge als schwer handhabbar. Benutzerfreundlichere Alternativen finden sich oft über Drittanbieter wie Hornetsecuritys 365 Multi-Tenant Manager für MSPs. Mit dieser Lösung können Sie eine eigene Standardkonfiguration speichern und Ihr individuelles Einstellungsset auf neue Kunden beim Onboarding übertragen.

ZUSAMMENFASSUNG

Effizienz im Onboarding ist entscheidend, um profitabel zu bleiben und Kunden mit Professionalität und Auftreten zu überzeugen. Durch den Einsatz von Tools wie Intune für die Gerätekonfiguration und Compliance sowie durch die Nutzung der Microsoft-Sicherheitsbaselines und Vorlagen können MSPs einen standardisierten und wiederholbaren Onboarding-Prozess kreieren. Ebenso wichtig sind jedoch sauber dokumentierte Standards, Checklisten und SOPs, damit alle Mitarbeiter einheitlich arbeiten.

Ebenso wichtig ist die Standardisierung von Portalkonfiguration und Sicherheitskontrollen während des Onboardings sowie deren langfristige Pflege. Microsoft liefert dafür Werkzeuge wie Sicherheitsbaselines und Tenant Configuration Management APIs. Viele MSPs werden jedoch Drittanbieter-Lösungen wie Hornetsecuritys 365 Multi-Tenant Manager für MSPs als benutzerfreundlicher und effektiver empfinden, wenn es darum geht, benutzerdefinierte Standardkonfigurationen zu erstellen, auszurollen und – wie wir in späteren Kapiteln noch sehen werden – die Sicherheitslage des Netzwerks aufrechtzuerhalten und zu aktualisieren.

Mit dem Fokus auf Automatisierung, Standardisierung und gründlicher Dokumentation können MSPs den Onboarding-Prozess optimieren, Ausfallzeiten minimieren und einen reibungslosen Übergang für neue Kunden sicherstellen. Das steigert nicht nur die Effizienz, sondern schafft auch Vertrauen in die erbrachten Services und führt letztlich zu einem erfolgreichen und positiven Onboarding-Erlebnis.

KAPITEL 3: MONITORING UND WARTUNG

Monitoring und Wartung sind seit jeher das Kerngeschäft vieler MSPs. Die Wartung unterstützt dabei, Probleme frühzeitig und proaktiv anzugehen, während automatisiertes Monitoring hilft, Veränderungen und Bedrohungen rechtzeitig zu erkennen. Angesichts der zunehmenden Bedeutung von Cybersicherheit, generativer KI und Compliance sind diese Aufgaben wichtiger denn je. Gleichzeitig haben sie noch nie so viel Aufmerksamkeit und Fachwissen erfordert wie heute.

Effizienz in Monitoring und Wartung zu erreichen ist anspruchsvoll. Schnell entsteht der Eindruck, dass alle Prozesse automatisiert werden sollten, insbesondere wenn man den aktuellen Diskussionen um KI folgt. In der Praxis sind menschliches Urteilsvermögen, Expertise und Erfahrung jedoch weiterhin unverzichtbar. Hinzu kommt die Frage, was passiert, wenn das Monitoring ein schwerwiegendes Problem erkennt. Genau an der Schnittstelle zwischen effizienter Automatisierung und einer wirksamen menschlichen Reaktion liegt für MSPs der Schlüssel zu wirtschaftlichem Erfolg. In vielerlei Hinsicht sind unsere Jobs heute anspruchsvoller und komplexer als früher. Das führt bei MSP-Inhabern und Mitarbeitern zu hoher Belastung. Klare Abläufe und Konzepte helfen dabei, effizient zu bleiben und die Arbeitslast wirksam zu steuern.

PROAKTIVE WARTUNG

Proaktive Wartung ist entscheidend, um Probleme zu verhindern, bevor sie kritisch werden. Herkömmliche Remote Monitoring and Maintenance (RMM)-Lösungen auf dem Markt sind häufig mit technischer Altlast belastet. Ihr Schwerpunkt liegt in erster Linie auf der Verwaltung von Software-Updates und der Suche nach Fehlern auf Hardwareebene. Das bleibt zwar wichtig, spielt heute aber eine weitaus geringere Rolle. Betriebssystem-Updates sind sicherer geworden, Hardware ist zuverlässiger, und Benutzer sind technisch versierter. Updates können so geplant werden, dass sie direkt im Betriebssystem und in den Anwendungen installiert werden.

Auch Hardwarefehler sind seltener geworden, weil austauschbare Komponenten und stark kühlungsbedürftige Systeme weniger verbreitet sind. Eine Studie von Backblaze über einen Zeitraum von fünf Jahren und mehrere tausend SSD-Laufwerke ergab eine Ausfallrate von unter 1 %.

MFG	Model	Size (TB)	# Drive count	# Avg. age (months)	# Drive days	Failures	AFR
HGST	HWS5C4848BLE648	4	187	188.24	17,194	8	0%
HGST	HUH728088ALE608	8	1,879	87.41	98,985	6	2.21%
HGST	HUH721212ALE608	12	2,615	69.57	239,677	9	1.37%
HGST	HUH721212ALE604	12	13,417	58.68	1,227,886	65	1.93%
HGST	HUH721212ALN604	12	9,985	74.97	912,361	189	4.36%
Seagate	ST8000NM002	8	8,987	106.89	824,787	27	1.19%
Seagate	ST8000NM008A	8	247	32.85	22,724	8	0%
Seagate	ST8000NM0055	8	13,351	95.55	1,224,448	53	1.58%
Seagate	ST18000NM0086	18	1,818	92.35	91,658	28	7.97%
Seagate	ST12000NM0007	12	1,085	69.87	91,835	13	5.17%
Seagate	ST12000NM0088	12	18,982	64.73	1,728,786	132	2.79%
Seagate	ST12000NM008J	12	1,819	14.12	91,723	2	0.88%
Seagate	ST12000NM001G	12	13,277	54.78	1,219,882	31	0.93%
Seagate	ST14000NM008J	14	392	11.85	31,852	4	4.58%
Seagate	ST14000NM001G	14	18,596	54.28	972,882	38	1.43%
Seagate	ST14000NM0138	14	1,286	56.57	117,131	22	6.86%
Seagate	ST16000NM001G	16	34,128	35.98	3,125,133	57	0.67%
Seagate	ST16000NM002J	16	463	33.86	42,581	8	0%
Seagate	ST24000NM002H	24	7,245	5.81	681,539	46	2.79%
Toshiba	MG87ACA14TA	14	37,463	58.28	3,448,851	116	1.23%
Toshiba	MG87ACA14TEY	14	978	35.12	85,538	8	3.41%
Toshiba	MG88ACA16TA	16	48,184	24.83	3,686,376	85	0.84%
Toshiba	MG88ACA16TE	16	6,177	43.84	553,332	16	1.06%
Toshiba	MG88ACA16TEY	16	5,145	44.61	462,943	215	16.95%
Toshiba	MG89ACA16TE	16	244	4.86	17,852	8	0%
Toshiba	MG18ACA28TE	28	18,823	7.88	1,416,127	21	0.54%
Toshiba	MG11ACA24TE	24	2,488	8.33	24,148	8	0%
WDC	WUH721414ALE6L4	14	8,663	55.33	794,781	28	0.92%
WDC	WUH721816ALE6L8	16	3,888	44.46	274,775	28	2.66%
WDC	WUH721816ALE6L4	16	26,681	29.85	2,439,889	65	0.97%
WDC	WUH722222ALE6L4	22	48,271	11.84	3,555,491	58	0.51%
Totals			328,348		29,431,783	1,258	1.55%

Abbildung 2: <https://www.backblaze.com/blog/how-reliable-are-ssds/>



Der Trend zu Laptops hat diese Entwicklung ebenfalls begünstigt. Während früher ein Hardware-Wechselzyklus von drei bis vier Jahren als Ziel galt, stellen viele MSPs heute fest, dass Geräte auch mit vier, fünf oder sogar sechs Jahren noch gut funktionieren.

Was bedeutet das für die Wartung? Möglichst viel sollte automatisiert werden, während das Monitoring auf Ausnahmen bei erfolgreichen Bereitstellungen achtet. Mit steigender Hardwarezuverlässigkeit sollte der Wartungsaufwand sinken.

AUTOMATISIERTES MONITORING

Während der Zeitaufwand für die Wartung gesunken ist, ist der Aufwand für das Monitoring trotz Automatisierung gestiegen. Warnmeldungen zu vollen Festplatten sind dank Cloud-Speicher seltener geworden, dafür haben Meldungen rund um Phishing, Identitäts- und Anwendungsaktivitäten stark zugenommen. Automatisiertes Monitoring ist zentral, um potenzielle Bedrohungen zu erkennen, denn es deckt die Geschäftskontinuität und Cybersicherheitsgefahren gleichermaßen ab. MSPs benötigen eine robuste und intelligente Monitoring-Lösung, um die Flut an Informationen aus Protokollen, Einstellungsänderungen und Malware-Indikatoren überhaupt bewältigen zu können. Das Monitoring-Programm ist das Rückgrat jeder Strategie zur Erkennung von Bedrohungen.

Das automatisierte Monitoring muss intelligent genug sein, um den Schweregrad einzelner oder kombinierter Änderungen zu bewerten. Microsofts integrierte Werkzeuge wie Intune für Geräteüberwachung, Sentinel für Alert-Management und Defender XDR für Incident-Tracking wirken zusammen als intelligente Monitoring-Lösung, die automatisiert reagieren, Aktivitäten abbilden und Warnungen versenden kann. Lösungen von Drittanbietern, wie Hornetsecuritys 365 Multi-Tenant Manager für MSPs und Business Protection-Pläne, verbinden mehrere Produkte mit KI-gestützter Intelligenz, um MSPs bessere Einblicke und automatisierten Schutz zu geben. Unabhängig vom gewählten Produkt sollte es sich um eine vollständige Tool-Suite handeln, die nicht nur überwacht, sondern bei Bedarf auch handelt.



Abbildung 3: Tenantübersicht im 365 Multi-Tenant Manager für MSPs

INCIDENT RESPONSE UND DISASTER RECOVERY

Die Komplexität von Incident Response und Disaster Recovery war noch nie höher. Angesichts der steigenden Lösegeldforderungen durch Cyberkriminelle sind Versicherungsgesellschaften und Behörden zunehmend in den Wiederherstellungsprozess eingebunden. Dadurch sind heute nicht nur technische Anforderungen zu berücksichtigen, sondern auch Compliance- und Versicherungsanforderungen, die in Incident-Response- und Disaster-Recovery-Pläne integriert werden müssen. Viele Versicherungen formulieren allgemeine Vorgaben wie „so bald wie möglich“, andere nennen feste Fristen wie 72 Stunden. Viele MSP-Techniker möchten sofort mit der Wiederherstellung beginnen, um den Betrieb schnellstmöglich wieder aufzunehmen. Cyberversicherungen verlangen jedoch oft zunächst nur die Eindämmung und fordern dabei als ersten Schritt die Kontaktaufnahme, damit ihre Spezialisten die Wiederherstellung begleiten können. Es gab viele Fälle, in denen übereifrige MSPs Systeme neu aufgesetzt haben, um das Geschäft möglichst schnell wieder in Gang zu bringen, und dadurch Beweise vernichteten, die gezeigt hätten, wie die Angreifer Zugriff erlangt haben und ob sie sich noch irgendwo im Netzwerk befinden. Schnelligkeit ist wichtig, aber zuerst muss verstanden werden, was genau passiert ist.

Ein kleiner KMU-Kunde von mir hatte einen Sicherheitsvorfall und ließ Benutzer-Laptops gegen unsere Empfehlung schnell neu aufsetzen, um rasch weiterarbeiten zu können. Wenige Tage später waren die Angreifer zurück und verteilten erneut Ransomware. Erst nach einem dritten Vorfall durfte ein DFIR-Team hinzugezogen werden. Die Untersuchung fand ein UEFI-Rootkit als Hintertür, das auch nach dem Re-Imaging aktiv blieb. Die einzige Lösung war die Anschaffung neuer Laptops für alle.

Hinzu kommen Compliance-Vorgaben, die bestimmte Meldepflichten vorsehen. Gleichzeitig investieren viele Unternehmen noch immer nicht in ausreichendem Maß in Prävention und Wiederherstellungsplanung. Cybersecurity-Bedrohungen haben das MSP-Geschäft ohne Zweifel deutlich schwieriger und komplexer gemacht.

DISASTER RECOVERY

Während all das geschieht, haben viele leider das Wesentliche bei der Wiederherstellung aus dem Blick verloren: das Backup. Es wirkt, als wäre Business Recovery vergessen worden, seitdem Daten in der Cloud gespeichert werden. Die Datensicherung war jedoch nie eine integrierte Standardfunktion der Cloud. Sie musste immer von einem Drittanbieter ergänzt werden. Die meisten Cloud-Anbieter bewerben ihre Backup-Funktionen, doch diese dienen in erster Linie ihnen selbst. Sollte bei ihnen ein Ausfall auftreten, können sie den Dienst und Ihre Daten für Sie wiederherstellen. Wenn Sie jedoch die Backup-Funktionalitäten wünschen, die ein Disaster-Recovery-Plan verlangt, einschließlich der Möglichkeit, zu verschiedenen Zeitpunkten in der Vergangenheit zurückzugehen, benötigen Sie einen Drittanbieter, der dies bereitstellt. Hornetsecurity bietet eine moderne [Backup-Lösung](#), die nicht nur Daten in Microsoft 365 umfasst, sondern auch Backups von VM-Servern und Endgeräten.

- » **Tenantfähigkeit:** Verwalten und überwachen Sie alle Microsoft 365-Organisationen und Backups von Windows-Endgeräten über eine zentrale, tenantfähige Online-Verwaltungskonsole.
- » **Benutzerfreundliches Backup-Dashboard:** Überwachen Sie Backup- und Wiederherstellungsaktivitäten, den Status der Backups und die jüngste Restore-Historie in einem zentralen Dashboard. Richten Sie Benachrichtigungen für erfolgreiche, fehlgeschlagene oder mit Warnungen versehene Backup-Status ein, erhalten Sie E-Mail-Benachrichtigungen oder tägliche Zusammenfassungen.
- » **Automatisierte Microsoft 365-Backups:** M365-Backups werden mehrmals täglich automatisch durchgeführt. Für Endgeräte können Backups so konfiguriert werden, dass sie alle 1 bis 24 Stunden erfolgen.
- » **Backup von lokalen und mobilen Endgeräten:** Sichern Sie jedes Endgerät, egal ob im Büro oder an einem beliebigen Ort weltweit, ohne dass ein VPN erforderlich ist.

- » **Endpunkt-Backup und Richtlinien:** Richtliniengesteuertes Backup auf Dateiebene für Windows-Desktops und -Laptops. Konfigurieren Sie Einstellungen für große Gruppen von Windows-Endgeräten, indem Sie Richtlinien einrichten, die Backup-Verzeichnisse, Cloud-Speicher, Frequenz und Aufbewahrungsdauer definieren.
- » **Daten jederzeit und überall sichern:** Sichern Sie jederzeit bestimmte Benutzer, Gruppen, Planner, SharePoint-/OneDrive-Dokumentbibliotheken und Endgeräte.
- » **Vier-Augen-Genehmigungsprinzip:** Eine zusätzliche Sicherheitsebene, die das Risiko von Datenverlusten durch Handlungen von unerfahrenen oder böswilligen Administratoren reduziert, indem sensible Aktionen wie das Löschen von Daten oder Änderungen an Unternehmenseinstellungen eine Freigabe durch mindestens einen zusätzlichen Administrator erfordern.

Eine so umfassende **Backup-Lösung** für die Notfallwiederherstellung ist in der heutigen Landschaft der Cyberkriminalität notwendig. Die Wahrscheinlichkeit, Daten wiederherstellen zu müssen, ist in den vergangenen Jahren parallel zur Cyberkriminalität gestiegen. Wichtig ist deshalb das regelmäßige Testen von Wiederherstellungsprozessen und dass der erste praktische Einsatz eines Wiederherstellungsprozesses nicht erst unter dem Druck eines echten Notfalls erfolgt.

INCIDENT RESPONSE

So gern man zu der Zeit zurückkehren würde, in der die Wiederherstellung aus einem Backup bereits als Reaktion auf einen Vorfall ausreichte, ist das heute nicht mehr realistisch. Die Komplexität ist inzwischen so stark gestiegen, dass MSPs einen klar definierten Incident-Response-Prozess brauchen. Moderne Incident Response umfasst sechs Bereiche – und die Wiederherstellung steht in dieser chronologischen Liste erst an fünfter Stelle.

- 1 EINDÄMMUNG:** Der erste Schritt besteht darin, den Sicherheitsvorfall einzudämmen, um weiteren Schaden zu verhindern. Dazu gehört betroffene Systeme zu isolieren, kompromittierte Konten zu deaktivieren und bösartige Prozesse zu stoppen. Idealerweise hat Ihre Monitoring-Anwendung die Bedrohung bereits erkannt, während Ihre Cybersecurity-Lösung schon damit begonnen hat, die Angriffskette zu unterbrechen.
- 2 BENACHRICHTIGUNG:** Danach müssen alle relevanten Stakeholder informiert werden. Bei KMU ist das in der Regel die Cyberversicherung, bei regulierten oder öffentlichen Organisationen die Rechtsabteilung und anschließend die zuständigen Aufsichts- oder Meldstellen. Diese müssen über den Vorfall informiert werden und bringen oft eigene Spezialisten in die Wiederherstellung ein.
- 3 UNTERSUCHUNG:** In dieser Phase kommen meist die Experten ins Spiel, die die Ursache und das Ausmaß der Kompromittierung genau ermitteln. Dazu gehört die Auswertung von Protokollen, die Identifikation kompromittierter Systeme und die Sicherung von Beweismitteln. Der MSP nimmt dabei häufig eine beratende Rolle ein, stellt Informationen für die Wiederherstellung bereit und übernimmt auch kommunikative Aufgaben. Als vertrauter Ansprechpartner kennt er die Verantwortlichen im Unternehmen, deren Arbeitsweise und die Geschäftsprozesse. Dadurch sind MSPs in einer wichtigen Position, um Kommunikationslücken zu schließen und realistische Erwartungen zu setzen. Sinnvoll ist es, schon vor einem Vorfall Kontakt zu einem oder mehreren Incident-Response-Dienstleistern aufzubauen, damit im Ernstfall nicht erst unter Zeitdruck nach Unterstützung gesucht werden muss.
- 4 BESEITIGUNG:** Anschließend wird der MSP oft eingebunden, um die Ursache des Vorfalls zu beseitigen. Dazu zählen etwa das Entfernen von Malware, das Schließen von Schwachstellen, das Neuaufrichten von Geräten und das Zurücksetzen von Passwörtern.
- 5 WIEDERHERSTELLUNG:** Wenn das Netzwerk bereits beschädigt wurde oder sich einzelne Bereiche nicht mehr zuverlässig als sicher einstufen lassen, muss der MSP betroffene Systeme und Daten aus Backups wiederherstellen und sicherstellen, dass alle Systeme wieder vollständig betriebsfähig sind. In manchen Fällen ist die Beschaffung neuer Hardware erforderlich.

- 6 NACHBEREITUNG DES VORFALLS:** Abschließend erstellen der MSP und alle weiteren Beteiligten einen Bericht und führen eine Nachbesprechung durch, um Erkenntnisse aus dem Vorfall festzuhalten und den Incident-Response-Plan für künftige Fälle zu verbessern. Gleichzeitig ist dies ein guter Zeitpunkt, um mit dem Kunden über Verbesserungen in Cybersicherheit und Resilienz zu sprechen, die zuvor für übertrieben oder zu teuer gehalten wurden. Ein schwerwiegender Vorfall macht oft sehr deutlich, wie wichtig belastbare Backup-Konzepte, phishing-resistente Authentifizierungsverfahren für alle Nutzer oder eine umfassende Cloud-Sicherheitslösung wie 365 Total Protection sind.

Sowohl das Unternehmen als auch der MSP gewinnen aus einem Vorfall in der Regel wichtige Erkenntnisse, die die Sicherheit des Unternehmensnetzwerks langfristig verbessern. Für den Kunden ist ein solcher Vorfall vor allem eine Geschäftsunterbrechung, deren technische Hintergründe er meist nicht vollständig einschätzen kann. Deshalb erwartet er vom MSP nicht nur die technische Wiederherstellung, sondern auch Einordnung, Sicherheit im Vorgehen und eine verständliche Erklärung der Maßnahmen in jeder Phase. Für beide Seiten ist dies eine Zeit hoher Belastung. Klare und verlässliche Kommunikation trägt daher entscheidend dazu bei, Missverständnisse und falsche Erwartungen zu vermeiden, die häufig Ursache späterer Unzufriedenheit sind.

Wenn der MSP den Disaster-Recovery-Plan professionell umsetzt, kann die Beziehung zum Kunden danach stärker sein als zuvor.

DIE RICHTIGE BALANCE ZWISCHEN EFFIZIENZ UND MENSCHLICHER EXPERTISE

All diese Aufgaben kosten Zeit, doch moderne Lösungen mit maschinellem Lernen und KI können MSPs spürbar entlasten. Voraussetzung dafür ist, dass ein Lösungsportfolio im Einsatz ist, das Automatisierung und KI-Funktionen umfasst und damit einen Teil des zeitlichen und fachlichen Aufwands des Helpdesks reduziert. Dann sollte der MSP in der Lage sein, einen Disaster-Recovery-Fall zu bewältigen, ohne seine regulären Aufgaben in den Bereichen Bereitstellung, Überwachung und Alarmierung zu vernachlässigen. Für erfolgreiches Monitoring und eine wirksame Wartung ist es entscheidend, die richtige Balance zwischen Effizienz und menschlicher Expertise zu finden.

Viele MSPs setzen mittlerweile verstärkt auf weniger qualifizierte Mitarbeiter, während Hersteller ihre Tools darauf ausgerichtet haben, Routineaufgaben zu vereinfachen und damit die Arbeitsbelastung für weniger erfahrene Mitarbeiter zu reduzieren. Dementsprechend benötigen MSPs qualifizierte Fachkräfte mit Erfahrung in Business Continuity und Disaster Recovery. Diese Mitarbeiter sollten nicht nur technisches Wissen mitbringen, sondern auch geschäftliche Zusammenhänge, Kommunikation, Cybersicherheit und Notfallwiederherstellung beherrschen. Weniger erfahrene Mitarbeiter werden weiterhin gebraucht, ihre Aufgaben sind jedoch toolbasiert und auf den Kundenservice ausgerichtet.

Am wichtigsten ist: Gerade die geringer qualifizierten Mitarbeiter sprechen am häufigsten mit Ihren Kunden. Sie beantworten Anrufe, übernehmen die Erstbewertung von Anfragen und leisten den Support auf erster Ebene. Diese Kontaktpunkte verdienen besondere Aufmerksamkeit, denn ein großer Teil der Kundenzufriedenheit hängt davon ab, wie gut sich der Kunde in Stressmomenten betreut fühlt.

Schulen Sie diese Mitarbeiter in Kommunikation und Empathie. Ein Kollege berichtete von einem Vorfall bei einem MSP, bei dem ein Anruf eines externen Nutzers einging, der sich über eine langsame und unzuverlässige Internetverbindung beschwerte. Die erste Reaktion des Technikers war die Frage: „Wo befinden Sie sich?“ Als der Nutzer antwortete, dass er auf dem Land sei, erwiderte der Techniker nur: „Das erklärt es“, bevor er auflegte.

ZUSAMMENFASSUNG

In diesem Kapitel wurden die zentralen Faktoren für mehr Effizienz von MSPs bei Monitoring und Wartung betrachtet. Dabei wurden die Bedeutung proaktiver Wartung, die Rolle automatisierter Überwachung, die Notwendigkeit klar definierter Incident-Response-Verfahren und Disaster-Recovery-Planung sowie die Balance zwischen Effizienz und menschlicher Expertise erläutert. Mit wirksamen Abläufen und klaren Konzepten können MSPs ihre Leistung steigern, Arbeitsbelastung reduzieren und ihre Profitabilität verbessern.

KAPITEL 4: KUNDENANPASSUNG

Kundenanpassung (engl. „Customization“) ist ein heikles Thema. MSPs müssen standardisieren, gleichzeitig aber anerkennen, dass jeder Kunde anders ist und vermeiden, Einheitslösungen einzusetzen, die jeder Wettbewerber replizieren könnte. Individuelle Anpassung an den jeweiligen Kunden hilft dabei, sich im Markt zu differenzieren, indem für jeden Kunden die passende technologische Lösung bereitgestellt wird. In diesem Kapitel unterscheiden wir zwischen benutzerdefinierter Bereitstellung und individueller Anpassung und betrachten, wann und warum beides sinnvoll ist.

WAS BEDEUTET KUNDENANPASSUNG?

Diese Frage wirkt zunächst simpel, ist aber entscheidend. Was ist eine benutzerdefinierte Bereitstellung und was ist eine Kundenanpassung? Durch eine Unterscheidung zwischen beiden verlieren wir das Ziel eines effizienten Betriebs nicht aus dem Blick.

EINE LÖSUNG ZUR BEREITSTELLUNG EINER BENUTZERDEFINIERTEN KONFIGURATION

Mit Hornetsecuritys 365 Multi-Tenant Manager für MSPs lässt sich auf der Grundlage der Standardarbeitsanweisungen (SOPs) schnell eine benutzerdefinierte Konfiguration erstellen. Dieses Tool ermöglicht es, die Konfiguration eines gesamten Tenant in kurzer Zeit bereitzustellen, sodass unser Design unmittelbar an alle von uns betreuten Tenants versendet wird. Jeder MSP sollte über eine benutzerdefinierte Bereitstellung verfügen, die die eigenen Standards widerspiegelt und zugleich empfohlene Baselines berücksichtigt.

Im Nachfolgenden finden Sie ein Beispiel dafür, wie dies aussehen könnte. Jedem Klienten in der untenstehenden Liste wird eine Vorlage zugewiesen, die unserer Standardkonfiguration für Klienten wie diesem entspricht.

Adempush AdemPush Offboard tenant NIST CSF 2.0 MBS Compliance Pack	USERS	GROUPS	POLICIES	SETTINGS	COMPLIANT
	10	16	26	60	100%
adventis.cre AdventisCre Offboard tenant NIST CSF 2.0 MBS Compliance Pack	USERS	GROUPS	POLICIES	SETTINGS	COMPLIANT
	14	11	29	46	100%
bell@mobite.ca BellMobileCa Offboard tenant Baseline security	USERS	GROUPS	POLICIES	SETTINGS	COMPLIANT
	0	0	26	53	100%

Abbildung 4: Hornetsecurity 365 Multi-Tenant Manager für MSPs

Durch die Verwendung von Vorlagen können wir unsere benutzerdefinierte Lösung effizient verwalten, indem wir Kunden der entsprechenden Vorlage zuordnen. Wenn Änderungen an der Vorlage vorgenommen werden, werden automatisch alle zugehörigen Kunden aktualisiert. So lässt sich eine benutzerdefinierte Konfiguration effizient bereitstellen.

ANPASSUNGEN EFFIZIENT UMSETZEN

Zusätzlich sollten Sie echte Anpassungen vornehmen. Bestimmte Bereiche eines Microsoft 365-Tenants lassen sich so gestalten, dass der Kunde erkennt, dass er in seiner eigenen Umgebung arbeitet, compliant bleibt und sicher arbeitet. Früher vermittelte der physische Server dieses Gefühl. Heute übernimmt diese Rolle die Anpassung der digitalen Umgebung.

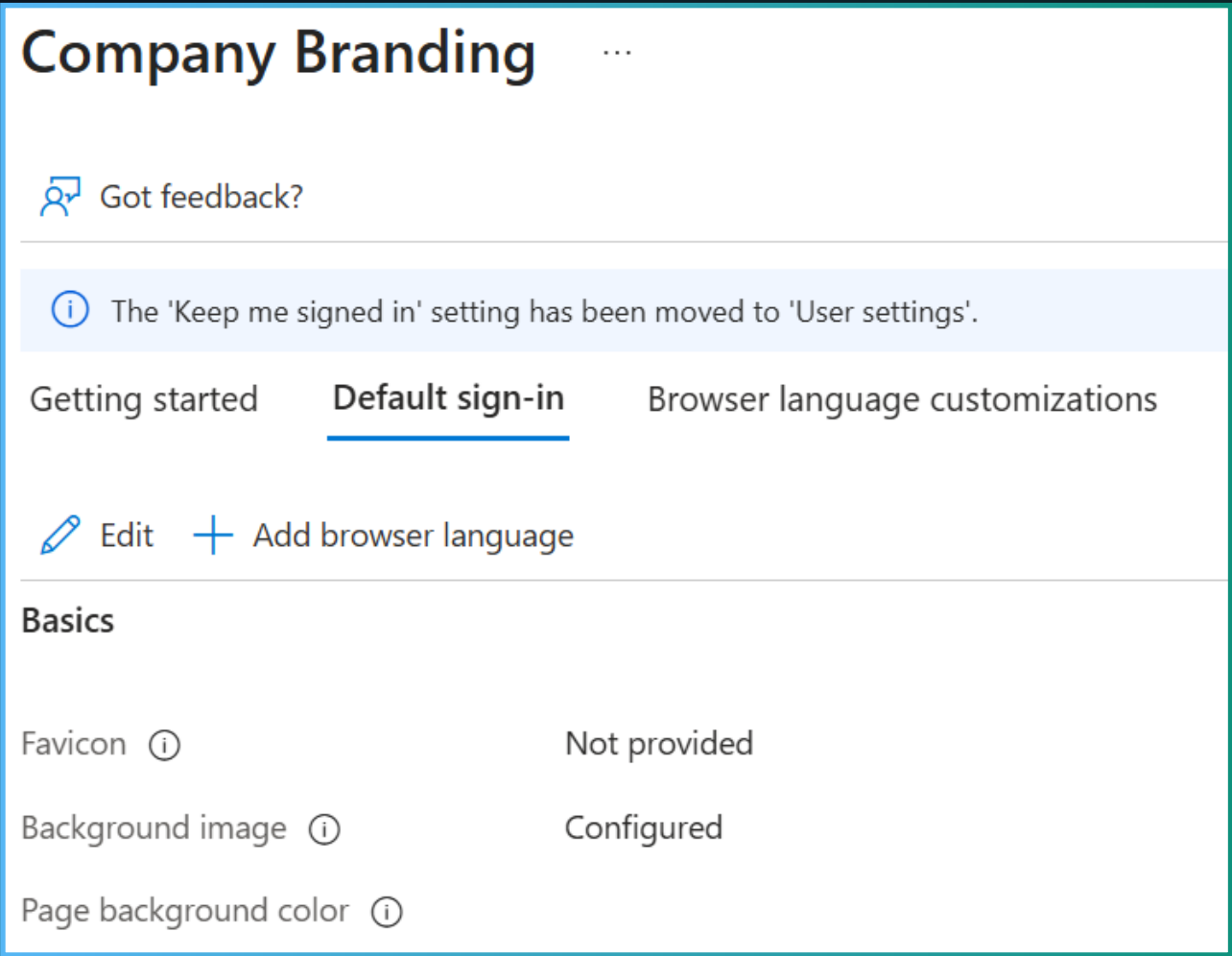


Abbildung 5: Personalisierung mithilfe eines vom Unternehmen genehmigtem Hintergrundbildes für die Anmeldung

Auch ohne physischen Server kann eine Microsoft 365-Bereitstellung durch Firmenlogo, Unternehmensnamen, Namen und Kontaktdaten des MSP-Supports sowie ein Hintergrundbild auf dem Anmeldebildschirm individuell angepasst werden. Solche Elemente helfen Benutzern zu erkennen, dass sie sich in ihrer Unternehmensumgebung befinden. Zusätzlich können sie auf Phishing aufmerksam machen, wenn gefälschte Anmeldeseiten das Corporate Branding nicht korrekt nachbilden. Für den MSP ist das zugleich ein Differenzierungsmerkmal gegenüber Wettbewerbern.

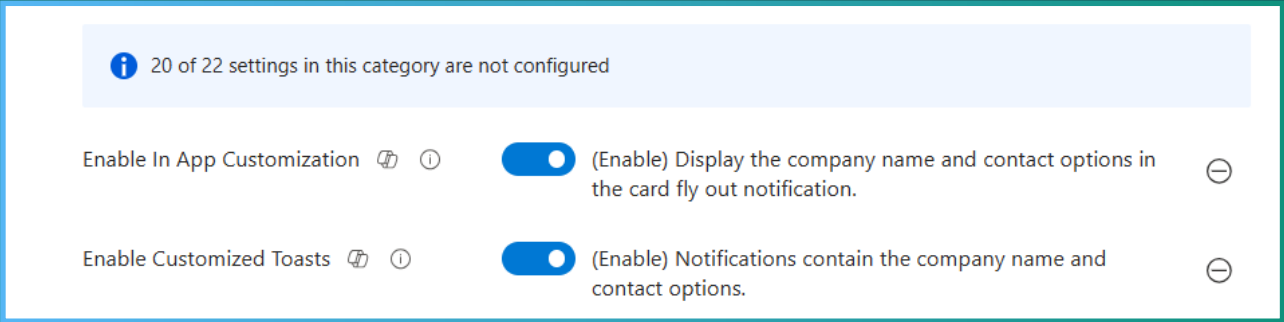


Abbildung 6: Anpassung von Toast-Pop-ups mit Firmennamen und Kontaktinformationen

Anpassungen können auch eine gewisse Standardisierung beinhalten, wenn sie für Gruppen von Kunden gilt. Haben Sie etwa mehrere Kunden, die Kreditkartendaten verarbeiten, benötigen alle Ihre PCI-Compliance-Richtlinie. Hornetsecuritys 365 Multi-Tenant Manager für MSPs erlaubt es, diese gezielt den passenden Tenants zuzuweisen. Genau wie bei Vorlagen für verschiedene Geschäftstypen können auch Vorlagen für Compliance- und Regulierungsanforderungen definiert und verwendet werden.

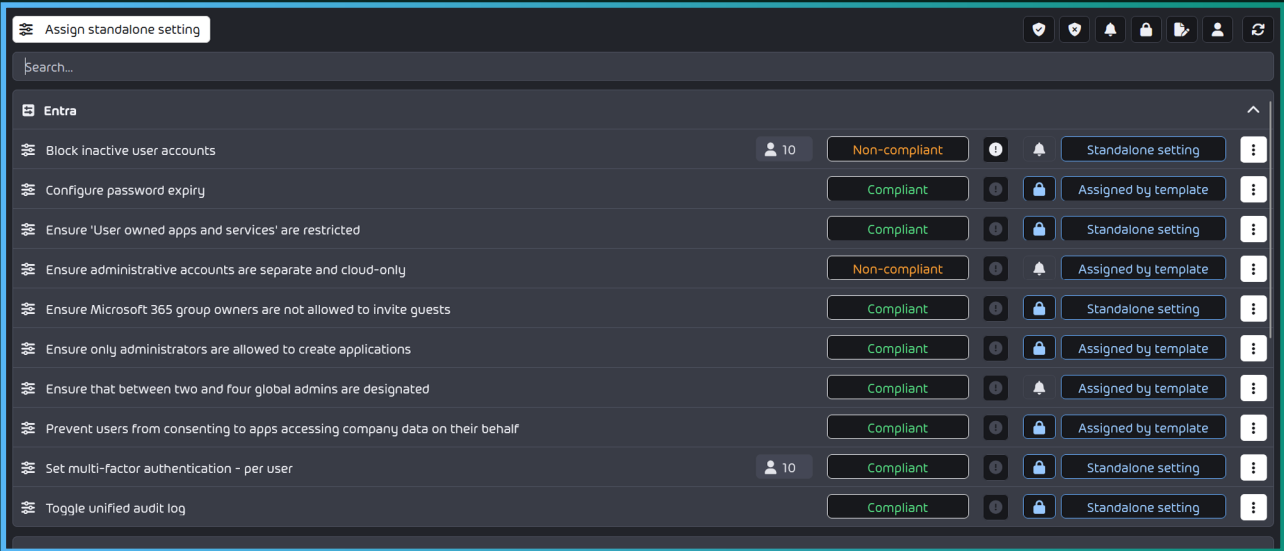


Abbildung 7: Vorlagen für die Einstellungen im 365Multi-Tenant Manager für MSPs



ZEITMANAGEMENT

Zeitmanagement ist der Schlüssel zur Effizienz eines MSP. Um effizient zu bleiben, müssen MSPs:

- » Die Erstbereitstellung mit Domainnamen und DNS-Einträgen konfigurieren
- » Eine angepasste Tenantkonfiguration bereitstellen
- » Konfigurationen zur Einhaltung von Vorschriften und regulatorischen Anforderungen für die richtigen Tenants bereitstellen
- » Spezifische geschäftliche Anpassungen vornehmen und Benutzererfahrungen konfigurieren

Die aufgewendete Zeit pro Aufgabe ist entscheidend. Ein effizienter MSP sollte höchstens 10 % seiner Zeit für die Bereitstellung von Tenants und 90 % für die Kundenanpassung aufwenden, einschließlich regulatorischer und Compliance-Anforderungen. Der Grund dafür ist simpel: Die individuelle Bereitstellung dient vor allem dem MSP, die Anpassung dagegen dem Kunden. Ein MSP sollte den Großteil seiner Zeit immer in kundenbezogene Arbeit investieren.

Bedenken Sie, dass die Realität Ihres Kunden oft ganz anders ist als Ihre eigene. Ein klassisches Beispiel aus meinem Geschäft: Ich suchte zu lange nach der kostengünstigsten Lösung, obwohl ich wusste, dass eine umfassendere Lösung langfristig besser wäre. Als ich beim Kunden nachfragte, sagte er knapp: „Ich habe Sie nicht gebeten, mir Geld zu sparen. Ich habe nach der besten Lösung gefragt.“ Prüfen Sie Ihre Annahmen, bevor Sie weitere Schritte unternehmen.

ÄNDERUNGSMANAGEMENT

Der letzte Bereich, den MSPs als Teil der Kundenanpassung meistern müssen, ist Änderungsmanagement. Werkzeuge sollten MSPs dabei helfen, den Änderungsverlauf nachzuverfolgen, doch es sind die SOPs, die dokumentieren, warum eine Änderung vorgenommen wurde. Fast jede Änderung, die ein MSP vornimmt, sollte auf eine bestehende Kundengruppe mit gemeinsamer Vorlage angewendet werden. Vermeiden Sie es, Einstellungen zu verwässern, um einem einzelnen Kunden in einer Vorlage entgegenzukommen. Eine gute Faustregel dabei ist, niemals eine Richtlinie auf der Grundlage einer Ausnahme zu erstellen. Wenn für einen einzelnen Kunden eine Ausnahme nötig ist, sollte er einer eigenen Vorlage zugewiesen werden. Ein effizienter MSP wird jedoch meist versuchen, alle Kunden an einen höheren Standard heranzuführen.



ZUSAMMENFASSUNG

Die Beherrschung von benutzerdefinierter Bereitstellung, kundenspezifischer Anpassung und Änderungsmanagement ist für MSPs entscheidend, um sich auf dem Markt abzuheben und ihren Kunden echten Mehrwert zu bieten. Durch die effiziente Bereitstellung kundenspezifischer Konfigurationen und die Pflege standardisierter Vorlagen können MSPs sicherstellen, dass sie individuelle Anforderungen ihrer Kunden erfüllen und gleichzeitig die operative Effizienz wahren. Gutes Zeitmanagement mit dem Schwerpunkt auf kundenbezogener Anpassung statt bloßer Bereitstellung führt zu höherer Kundenzufriedenheit und einem stärkeren Leistungsversprechen auf dem Markt.

365 TOTAL PROTECTION

AI-POWERED, ALL IN ONE M365 SECURITY, BACKUP & GRC

 365 MULTI-TENANT
MANAGER FOR MSPS

STOP MANUALLY MANAGING M365 TENANTS
AND START SAVING YOUR TIME!

PLAN
4

INCLUDES 1 + 2 + 3

 SECURITY
AWARENESS

 PERMISSION
MANAGEMENT

 DMARC
REPORTING &
MANAGEMENT

POWERED BY AI CYBER ASSISTANT

 AI RECIPIENT
VALIDATION

 TEAMS
PROTECTION

 AI EMAIL
SECURITY
ANALYST

PLAN
3

INCLUDES 1 + 2

 AUTOMATIC
BACKUP
OF M365 DATA

 GRANULAR
RECOVERY WITH
END USER SELF
SERVICE

 UNLIMITED
STORAGE IN ONE
ALL-INCLUSIVE FEE

PLAN
2

INCLUDES 1 + 2

 ADVANCED
THREAT
PROTECTION

 EMAIL
ARCHIVING

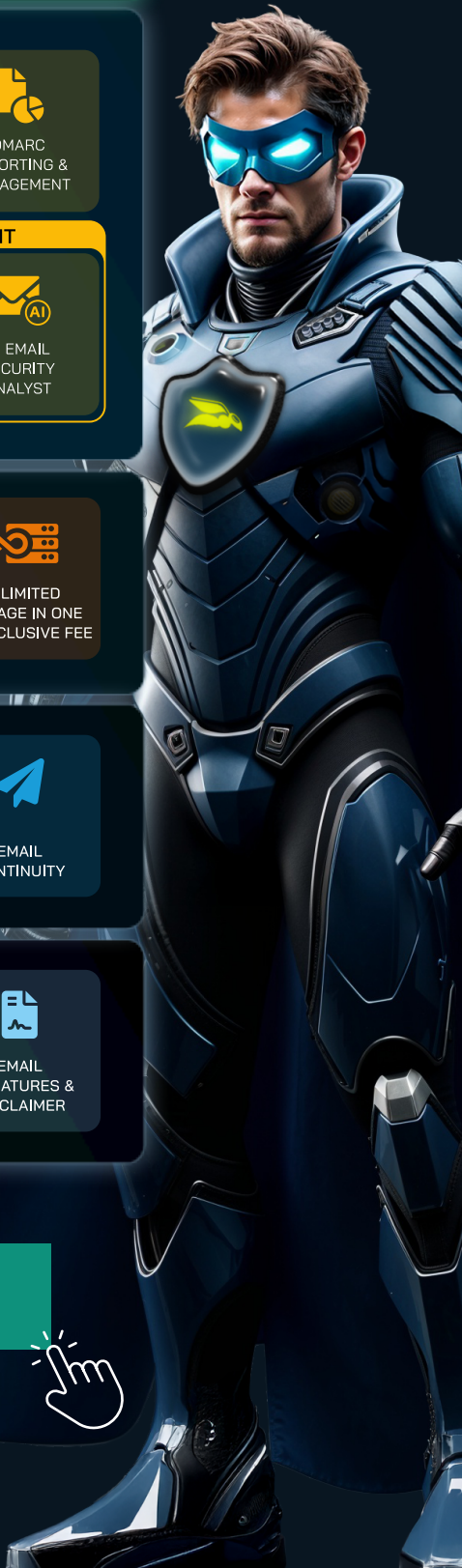
 EMAIL
CONTINUITY

PLAN
1

 SPAM &
MALWARE
PROTECTION

 EMAIL
ENCRYPTION

 EMAIL
SIGNATURES &
DISCLAIMER



KOSTENLOS TESTEN

KAPITEL 5: CYBERSICHERHEIT

Für MSPs und ihre Kunden gibt es derzeit kaum ein wichtigeres Thema als Cybersicherheit, abgesehen von generativer KI, die sich stark mit der Cybersicherheit überschneidet. Das Thema Cybersicherheit verdient eigentlich ein eigenes E-Book. Es sind zahlreiche Einstellungen und kontinuierliche Wartung erforderlich, um Cyberkriminellen immer einen Schritt voraus zu sein und Kunden zu schützen. In diesem Kapitel liegt der Schwerpunkt weniger auf spezifischen Einstellungen als auf der Frage, wie MSPs in einer sich schnell verändernden Sicherheitslandschaft effizient und profitabel bleiben.

Bei der Überlegung, wie der Schutz der Netzwerke, für die MSPs verantwortlich sind, zu bewerkstelligen ist, muss der gesamte Werkzeugkasten genutzt werden.

SCHWACHSTELLEN VERSTEHEN

Microsoft stellt Bedrohungsberichte von eigenen Analysten im Bereich „[Threat Analytics](#)“ von [Defender](#) bereit, die Aufschluss darüber geben, wie konkrete Bedrohungen funktionieren, und sind dabei detailliert, aber gut verständlich. Sie beginnen mit einer Zusammenfassung und gehen dann auf die Funktionsweise der Bedrohung ein. Die Berichte sind für alle Nutzer einer M365-Lizenz verfügbar; die Verwendung der Defender-Suite ist dabei nicht erforderlich.

A

Activity Profile: Multi-stage code of conduct phishing campaign with PDF attachment leads to AiTM token compro...

Category: Activity | Published: May 5, 2026 12:27 AM | Last updated: May 5, 2026 12:27 AM

Phishing

Overview

Analyst report

Related incidents

Impacted assets

Endpoints exposure

Recommended actions

Indicators (Preview)

Executive summary

Please take a moment to provide feedback on this Threat Intelligence profile.

Between April 14 and 16, 2026, Microsoft Defender Research observed a large-scale phishing campaign targeting over 35,000 users across more than 13,000 organizations, primarily in the United States, using code of conduct-themed lures and PDF attachments to initiate a multi-stage credential harvesting flow. The campaign leveraged Alibaba Cloud Direct Mail to distribute fully authenticated messages from attacker-controlled domains, enhancing deliverability and legitimacy. The phishing attack chain directed users through a multi-step attack chain incorporating CAPTCHA gating and intermediate staging pages before ultimately being presented with a legitimate Microsoft sign-in experience as part of an *adversary-in-the-middle (AiTM)* phishing framework. This approach enabled attackers to capture authentication tokens and compromise user accounts while evading traditional detection mechanisms.

Microsoft Defender XDR detects suspicious activities related to AiTM phishing attacks and their follow-on activities. Organizations can defend against financial fraud initiated through phishing emails by educating users about phishing lures, configuring essential email security settings, and encouraging users to employ web browsers that support SmartScreen. Organizations can also enable network protection, which lets Windows use SmartScreen as a host-based web proxy. See the **Recommendations** section for details.

Abbildung 8: Zusammenfassung zu Beginn des detaillierten Bedrohungsberichts

Weitere Registerkarten zeigen, wie sich die Bedrohung auf den eigenen Tenant auswirkt und welche Maßnahmen zum Schutz des Netzwerks möglich sind. Ein Klick auf nicht erledigte Aufgaben führt direkt zu den Anleitungen für die Umsetzung des Schutzes.

Overview

Analyst report

Related incidents

Impacted assets

Endpoints exposure

Recommended actions

Indicators (Preview)

Perform these actions to address this threat and improve your overall posture. For a broader assessment and more recommended actions, view your secure score.

There are new permissions options available for Secure Score. You can now configure users' Secure Score data visibility based on data source. [Learn more about this change.](#)

Configure in URBAC

Export

6 items

Search

Filter

Group by

Rank	Recommended action	Score impact	Points achieved	Status	Regressed	Have license?	Category	Product	Last synced
83	Ensure Safe Links for Office Applications is Enabled	+0.19%	0/3	To address	No	Yes	Apps	Defender for Office	5/8/2026
155	Create zero-hour auto purge policies for malware	+0.38%	5.97/6	To address	No	Yes	Apps	Defender for Office	5/8/2026
157	Ensure Safe Attachments policy is enabled	+0.32%	4.97/5	To address	No	Yes	Apps	Defender for Office	5/8/2026
169	Set Microsoft Defender SmartScreen Microsoft Edge site and download checkir	+0.57%	9/9	Completed	No	No	Device	Defender for Endpoint	5/10/2026
257	Create zero-hour auto purge policies for phishing messages	+0.19%	3/3	Completed	No	Yes	Apps	Defender for Office	5/8/2026
268	Create zero-hour auto purge policies for spam messages	+0.06%	1/1	Completed	No	Yes	Apps	Defender for Office	5/8/2026

Abbildung 9: Liste empfohlener Maßnahmen zum Schutz des Netzwerks

Im Microsoft Defender-Portal werden außerdem Sicherheitslücken aufgelistet, die keiner konkreten Bedrohung zugeordnet sind, von denen es sehr viele gibt. Viele sind theoretisch möglich, werden aber in der Praxis nicht aktiv ausgenutzt. In der Liste der Sicherheitsempfehlungen (Abb. 10) kennzeichnen rote Käfersymbole aktiv ausgenutzte Schwachstellen, graue Symbole dagegen potenzielle Schwachstellen.

Name	Devices Score impact	Exposed critical device	Category	Threats	Exposed devices	Remediation a
Block executable files from running unless they meet a prevalence, age, or trusted list criterion	+0.94%	3	Security controls (Attack Surface Reduction)		109 / 109	0
Block use of copied or impersonated system tools	+0.94%	3	Security controls (Attack Surface Reduction)		109 / 109	0
Block rebooting machine in Safe Mode	+0.94%	3	Security controls (Attack Surface Reduction)		109 / 109	0
Block outbound network connections from Microsoft HTML Application Host (mshta.exe)	+0.84%	3	Network		110 / 110	0
Disable NTLM authentication for Windows workstations	+0.84%	3	Network		110 / 110	0
Set User Account Control (UAC) to automatically deny elevation requests	+0.84%	3	Operating system		109 / 109	0

Abbildung 10: Sicherheitsempfehlungen mit Kennzeichnung aktiv ausgenutzter Schwachstellen

Durch diese beiden Werkzeuge kann ein effizienter MSP seine Sicherheitswartung auf die Schwachstellen konzentrieren, die für Kunden mit höherer Wahrscheinlichkeit relevant sind.

Angesichts der Menge an Schwachstellen und Angreifern scheint Cybersicherheit oft ein unlösbares Problem zu sein. Doch mit den beschriebenen Werkzeugen lässt sich der Umfang sinnvoll eingrenzen und die Absicherung der Kundennetzwerke pragmatisch angehen.

BASELINES

Ein weiteres Hilfsmittel, das bei der Optimierung der Cybersicherheit unterstützt, sind Baselines. Microsoft stellt Sicherheitsbaselines für Windows, Edge, Windows 365, Defender for Endpoint und Microsoft 365-Apps bereit.

Security baselines ↑	Version
Advanced Security Baseline for HoloLens 2	Version 1
Microsoft 365 Apps for Enterprise Security Baseline	Version 2306
Microsoft Defender for Endpoint Security Baseline	Version 24H1
Security Baseline for Microsoft Edge	Version 139
Security Baseline for Windows 10 and later	Version 25H2
Standard Security Baseline for HoloLens 2	Version 1
Windows 365 Security Baseline	Version 24H1

Abbildung 11: Microsoft Security Baselines, die in Intune bereitgestellt werden

Sie können diese Baselines direkt verwenden, doch sie sind häufig sehr streng und für viele Unternehmen schwer umsetzbar. Sinnvoller ist meist, die Einstellungen zu prüfen und auf dieser Basis einen eigenen Standard zu entwickeln. Haben Sie diesen Standard einmal definiert, können Sie ihn tenantübergreifend einsetzen.

Dafür benötigen Sie allerdings ein Drittanbieter-Tool wie Hornetsecuritys 365 Multi-Tenant Manager für MSPs, um Ihre Standards allen von Ihnen betreuten Netzwerken zuzuweisen. Die Vorlagenfunktion ist hier besonders nützlich.

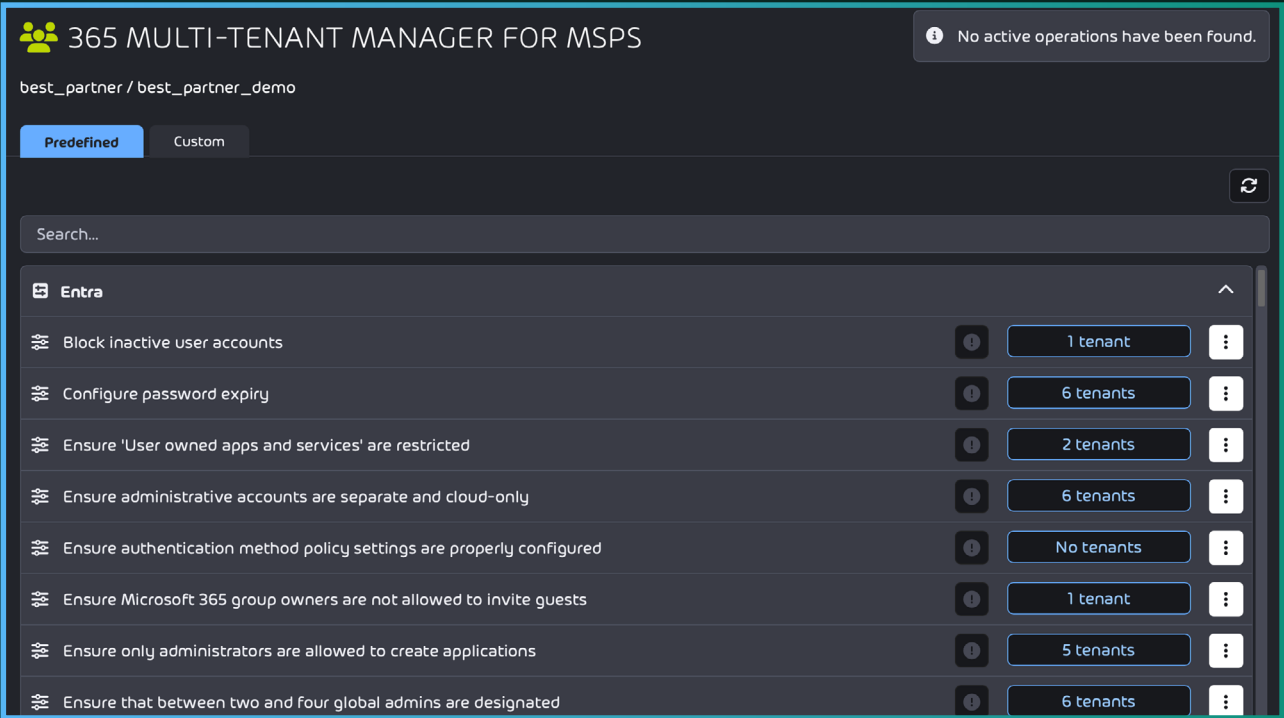


Abbildung 12: Einstellungsbibliothek von Hornetsecuritys 365 Multi-Tenant Manager für MSPs

E-MAIL-SICHERHEIT

Erstaunlicherweise gibt es keine Baseline für die E-Mail-Sicherheit. Angesichts des starken Anstiegs von Business Email Compromise (BEC) als Einfallstor für Netzwerkangriffe wäre das naheliegend. Microsoft begegnet diesem Problem stattdessen mit vordefinierten Vorlagen für E-Mail-Sicherheitsrichtlinien in Defender for Business.

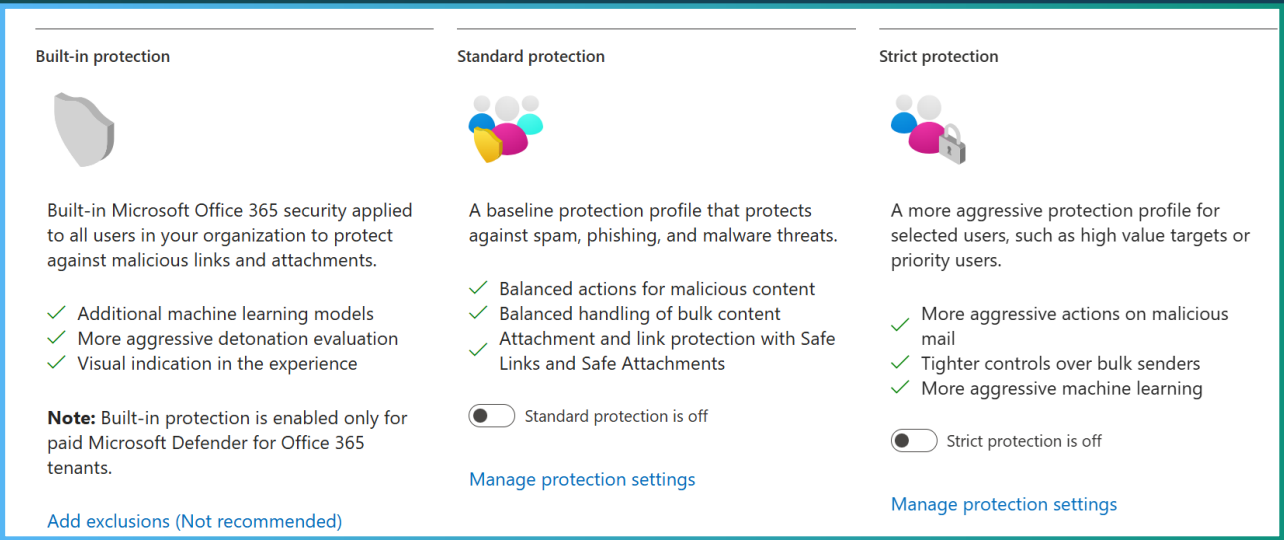


Abbildung 13: ordefinierte Sicherheitsrichtlinien für E-Mail

Es gibt kaum eine wichtigere Sicherheitsmaßnahme als eine vollständige E-Mail-Sicherheitslösung. Kriminelle setzen Phishing, Spear Phishing, Quishing und andere Methoden des Social Engineering ein, um sich Zugang zu einem Netzwerk zu verschaffen. Unternehmen müssen heute beim Umgang mit E-Mails äußerste Vorsicht walten lassen. Generative KI hat das Imitieren von Benutzern, das Formulieren überzeugender Inhalte und das Tarnen betrügerischer URLs auf ein neues Niveau gehoben. Dagegen hilft nur ein umfassendes E-Mail-Sicherheitstool und eine gewisse Toleranz gegenüber Fehlalarmen. Die Kombination aus Microsoft-Vorlagen und [Hornetsecuritys 365 Total Protection](#) ist dafür ein wirkungsvoller Ansatz.

Grundlage wirksamer E-Mail-Sicherheit sind die drei E-Mail-Protokolle Sender Policy Framework (SPF), Domain-based Message Authentication (DMARC) und Domain Keys Identified Mail (DKIM). Stellen Sie sicher, dass diese für jede E-Mail-Domain Ihrer Kunden korrekt konfiguriert sind, beispielsweise mit unserem Service [DMARC Manager](#).

INTUNE UND RICHTLINIEN FÜR EINGESCHRÄNKTEN ZUGRIFF (CONDITIONAL ACCESS)

Intune ist, wie bereits erwähnt, ein hervorragendes Konfigurationswerkzeug. Es überträgt Ihre Konfigurationen und Anwendungen auf Geräte in Ihrem Netzwerk und ermöglicht so detaillierte Kontrolle über verbundene Geräte, was an sich bereits eine Sicherheitsmaßnahme ist. In Kombination mit Conditional Access-Regeln von Entra können wir den Netzwerkzugriff auf Geräte beschränken, die tatsächlich eingebunden sind. Angreifer registrieren in kompromittierten Umgebungen durchaus eigene Geräte (Smartphone oder Laptop), um späteren Zugriff zu sichern. Deshalb ist es sinnvoll, den Zugriff nur für Entra- oder domänengebundene Geräte zu erlauben und die Geräteregistrierung zusätzlich an MFA oder phishingresistente Authentifizierung zu koppeln.

Eine weitere wirksame Richtlinie beschränkt den Zugriff auf unterstützte Plattformen. Wenn Sie in Ihrem Netzwerk beispielsweise Linux, Mac oder ältere Windows-Versionen nicht nutzen, sollten diese blockiert werden. Ziel ist es, Angreifern ihre Arbeit so schwer wie möglich zu machen.

Block access for unknown or unsupported device platform

Users will be blocked from accessing company resources when the device type is unknown or unsupported.

[Learn more](#)

Require compliant or hybrid Azure AD joined device for admins

Require privileged administrators to only access resources when using a compliant or hybrid Azure AD joined device.

[Learn more](#)

Abbildung 14: Einschränkung der zulässigen Betriebssystemplattformen mithilfe von Intune

Erweiterte Microsoft 365-Lizenzpakete wie Entra ID P2 enthalten außerdem Funktionen wie „Risky User“, „Risky Sign-In“ und „Risky Device“, die in Richtlinien integriert werden können, um nur bekannte, sichere Benutzer und Geräte zuzulassen.

Die Verwaltung von Conditional Access-Richtlinien über alle Kundentenanten hinweg ist essenziell, aber manuell sehr zeitaufwendig. Hornetsecuritys 365 Multi-Tenant Manager für MSPs unterstützt hier mit skalierbarer Anpassung und Bereitstellung von CA-Richtlinien.

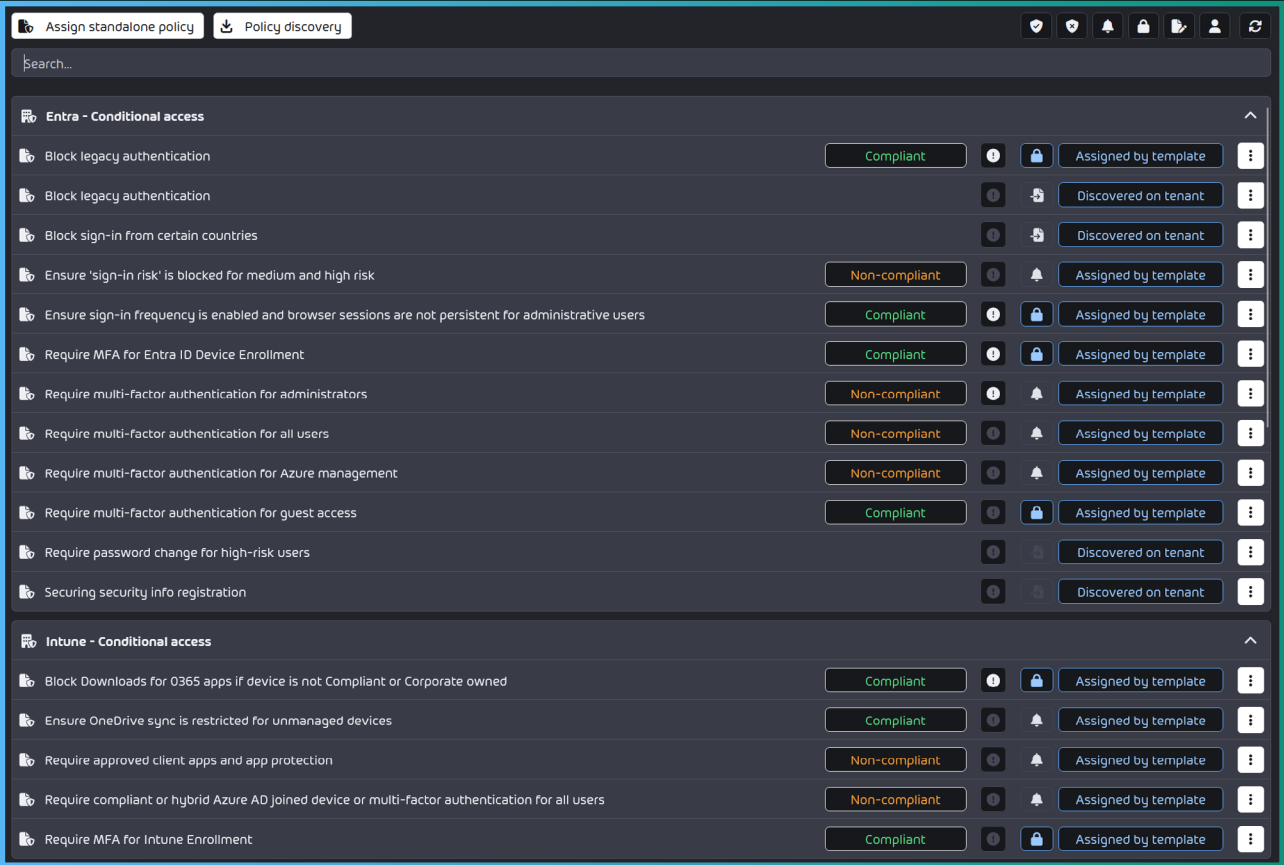


Abbildung 15: Bibliothek für Conditional Access-Richtlinien im 365 Multi-Tenant Manager für MSPs

AUTOPILOT, LIGHTHOUSE UND BACKUP

Neben den Tools, mit denen Sicherheitskonfigurationen ermittelt und festgelegt werden können, sollten auch Autopilot, [Microsoft 365 Lighthouse](#) (oder ein gleichwertiges Produkt eines Drittanbieters) und eine Backup-Lösung Teil der Sicherheitsstrategie sein. Autopilot dient dazu, Geräte, die zu Ihrer Domäne gehören, eindeutig zu identifizieren und Ihnen die Kontrolle über das Gerät ab dem ersten Einschalten zu gewähren. Lighthouse hilft bei der Verwaltung von Einstellungen über mehrere Kunden hinweg, sofern kein Drittanbieter dafür genutzt wird. Backup stellt Business Continuity sicher, wenn alles andere versagt.

Gerade dieser Business-Continuity-Baustein scheint bei vielen MSPs aus dem Blickfeld geraten zu sein. Ein übersichtliches Dashboard, das den Backup-Status aller Tenants zeigt, ist eine effiziente Möglichkeit, den Überblick über den Status der Backups zu behalten.

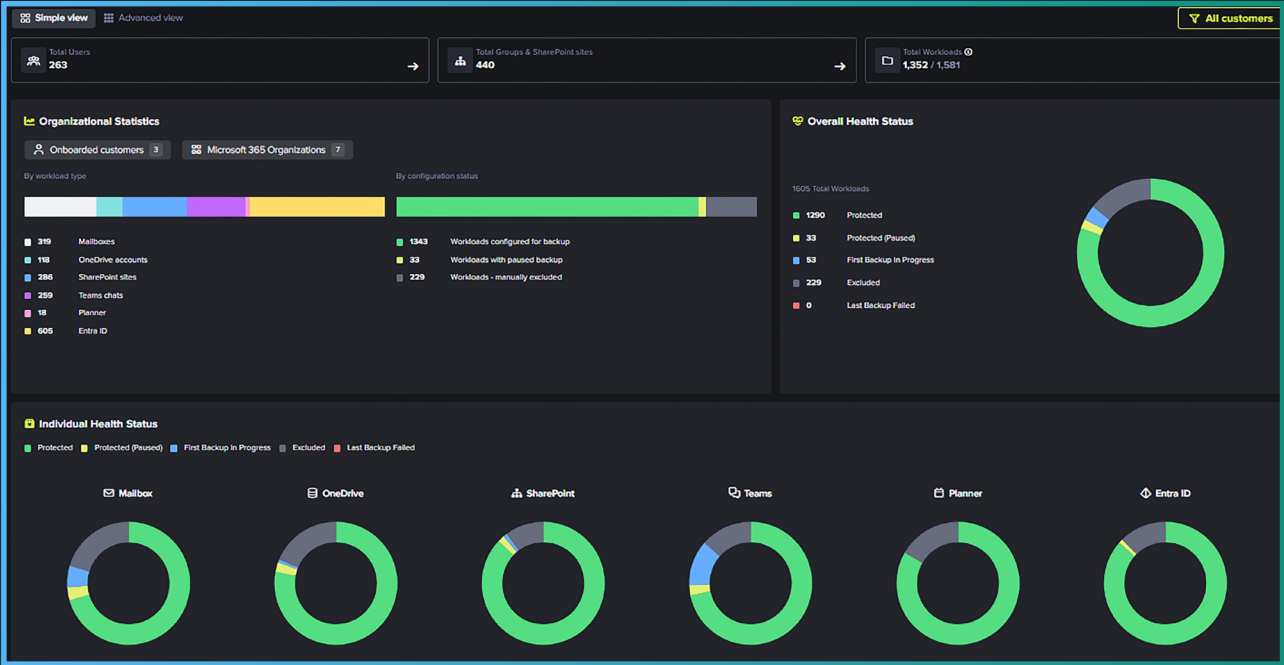


Abbildung 16: Dashboard zum Backup-Status von Hornetsecurity 365 Total Backup

Um den Business-Continuity-Prozess zu vervollständigen, sollte der MSP mindestens vierteljährlich Testwiederherstellungen durchführen. Denn ein Backup ist nur dann wertvoll, wenn es erfolgreich wiederhergestellt werden kann.

Der Schlüssel zum Umgang mit Cybersicherheit für Ihre Kunden ist Transparenz. Mit einem optimierten System (wie Microsoft Sentinel) kann innerhalb weniger Minuten festgestellt werden, wenn jemand eine neue Conditional Access-Richtlinie anlegt, eine neue MFA-Methode für sein Konto hinzufügt oder Opfer eines MFA-Fatigue-Angriffs geworden ist (so viele Anforderungen, dass der Endnutzer schließlich einfach zustimmt, damit die Meldung verschwinden). Diese nahezu in Echtzeit verfügbare Sichtbarkeit ermöglicht es, kleine Vorfälle einzudämmen, bevor sie sich zu großen Sicherheitsverletzungen entwickeln.

ZUSAMMENFASSUNG

Die Bedrohungslandschaft entwickelt sich ständig weiter. IT-Verantwortliche, die sich auf kleine Unternehmen konzentrieren, müssen in ihrem Cybersicherheitsansatz wachsam und proaktiv bleiben. Mit den in diesem Kapitel beschriebenen Werkzeugen und Strategien können sie die Netzwerke und Daten ihrer Kunden wirksam schützen und dabei effizient und profitabel bleiben. Cybersicherheit ist kein einmaliges Projekt, sondern ein fortlaufender Prozess, der kontinuierliches Lernen und Anpassen erfordert.



365 TOTAL BACKUP



**JETZT M365-DATEN
SCHÜTZEN**

KAPITEL 6: ANBIETERVERWALTUNG

Es gibt mehrere Wege, die Verwaltung von Anbietern in einem MSP anzugehen. Sollten Sie auf mehrere erstklassige Anbieter setzen oder sich für einen einzigen Anbieter entscheiden? Auf den ersten Blick klingt die Entscheidung einfach, ist sie aber nicht. Wenn Effizienz das Ziel ist, müssen viele Faktoren berücksichtigt werden. Es muss eine Entscheidung getroffen werden, die operative Effizienz für den MSP mit einer leistungsstarken Lösung für Kunden vereint. Für solche komplexen Entscheidungen helfen strukturierte Prozesse wie Vergleichstabellen oder SWOT-Analysen. In diesem Kapitel werden wir beide Ansätze untersuchen.

DER ANSATZ DER VERGLEICHSTABELLE

Vor vielen Jahren, als die Cybersicherheitslandschaft noch weniger komplex und Sicherheitsanforderungen nicht so umfassend waren, habe ich ebenfalls den „Best-of-Breed“-Ansatz bevorzugt. Damals war diese Entscheidung noch gut handhabbar, weil sie häufig bedeutete, mit nur zwei Herstellern zu arbeiten und der operative Aufwand überschaubar blieb. Mit der Weiterentwicklung der Bedrohungslage hat sich meine Sichtweise jedoch verändert. Heute erfordert eine konsequente „Best-of-Breed“-Strategie nicht länger zwei sorgfältig ausgewählte Anbieter zu verwalten, sondern eine wachsende Anzahl an Produkten, Portalen, Verträgen und Supportbeziehungen zu koordinieren. Gleichzeitig sind die funktionalen Unterschiede zwischen Lösungen verschiedener Anbieter geringer geworden, da sich Technologien in diesem Bereich deutlich weiterentwickelt haben. Was früher einen klaren technischen Vorteil bot, führt nun zunehmend zu höher operativer Komplexität.

Diese Entscheidung war nie nur eine Wahl zwischen einem Anbieter und mehreren. Sie war immer mit Kompromissen verbunden. Verwaltungsaufwand, Kosten, Integration, Innovationskraft und zunehmend Anbieterabhängigkeit müssen berücksichtigt werden.

Faktor	Single-Vendor-Ansatz	Best-of-Breed-Ansatz
Verwaltungsaufwand	Einfach	Komplex
Kosten	Einsparungen?	Höhere Kosten
Integration	Nahtlos	Herausfordernd
Innovation	Begrenzt?	Hoch
Anbieterabhängigkeit	Hoch	Niedrig?

Beim Best-of-Breed-Ansatz ist die Komplexität immer höher. Mehrere Verwaltungsportale müssen überwacht, mehrere Anbieter bezahlt und mehr Verträge im Blick behalten werden, was den Aufwand für MSPs erhöht. Integration ist oft schwierig oder gar nicht möglich. Gleichzeitig binden Hersteller Kunden immer häufiger an lange oder belastende Vertragslaufzeiten.

Hinzu kommt die Unsicherheit über die Grenzen zwischen den Produkten verschiedener Anbieter. Oft ist unklar, wo der Einfluss des einen endet und der des anderen beginnt. Wer zu viele Anbieter kombiniert, riskiert ungewollte Lücken.

SWOT-ANSATZ

Die SWOT-Analyse bewertet Stärken, Schwächen, Chancen und Risiken und eignet sich gut für viele Entscheidungsaufgaben. Die Anwendung von SWOT kann auch dabei helfen, die beiden Ansätze bei der Verwaltung von Cybersicherheitsanbietern zu veranschaulichen.

SINGLE-VENDOR-SWOT

- » **Stärken:** vereinfachtes Management, geringere Komplexität, einheitliche Benutzererfahrung, potenzielle Kosteneinsparungen.
- » **Schwächen:** Einheitslösung, Anbieterabhängigkeit, begrenzte Innovation.
- » **Chancen:** optimierte Abläufe, einfacherer Support.
- » **Risiken:** Abhängigkeit von einem Anbieter, potenzielle Sicherheitslücken.

BEST-OF-BREED-SWOT

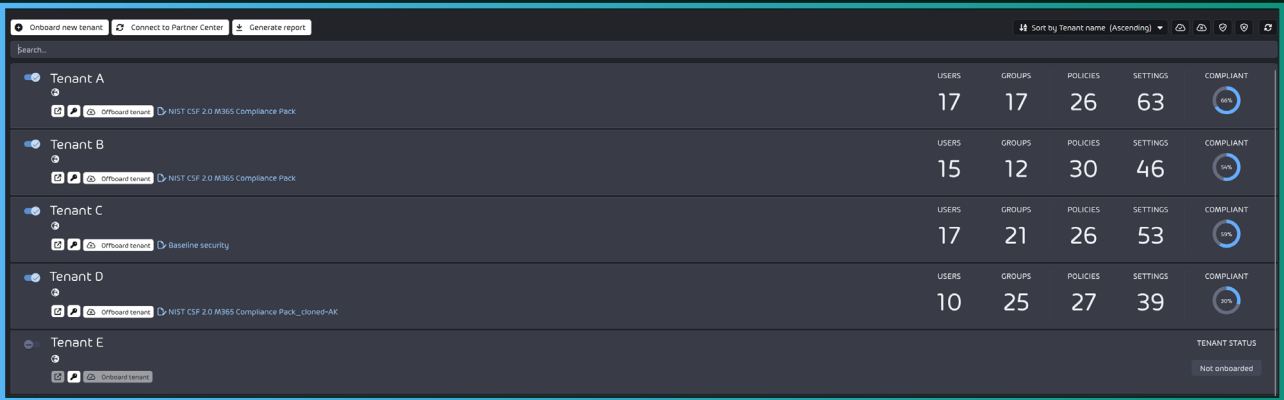
- » **Stärken:** spezialisierte Expertise, Flexibilität, geringere Anbieterabhängigkeit.
- » **Schwächen:** komplexes Management, höhere Kosten, Integrationsherausforderungen.
- » **Chancen:** Zugang zu neuesten Technologien, maßgeschneiderte Lösungen.
- » **Risiken:** erhöhte Komplexität, unbekannte Lücken zwischen Anbietern.

Eine Auswertung der Literatur zur Nutzung von MSP-Anbietern zeigt, dass bei den größten MSPs bis zu 70 Anbieter involviert sein können, während es bei einem durchschnittlichen MSP etwa sieben waren. Gleichzeitig ist ein Trend zur Konsolidierung der Anbieter sichtbar. Dies ist zum Teil auf den allgemeinen Konsolidierungstrend im Herstellermarkt selbst zurückzuführen, zum Teil aber auch auf das Streben nach betrieblicher Effizienz, nachdem erkannt wurde, dass MSPs viele Anbieter weder operativ beherrschen noch ihre Mitarbeiter auf so viele Lösungen schulen können. Die wachsende Komplexität der Cybersicherheit zwingt MSPs dazu, eine Auswahl treffen zu müssen.

Auch wenn ein einzelner Anbieter selten ausreicht, kann es sinnvoll sein, zwei Anbieter als Standard zu definieren. Microsoft ist einer davon. Microsoft hat stark in Sicherheit investiert und viele Sicherheitsprodukte in Microsoft 365 integriert. Gleichzeitig ist der Ansatz eher auf Unternehmen mit spezialisierten Sicherheitsteams ausgerichtet. Der typische MSP ist kleiner und arbeitet mit Security-Generalisten, die mit der gesamten Bandbreite der Cybersicherheit vertraut sein müssen. Dies ist nicht die Stärke von Microsoft. Deshalb ist ein zweiter Anbieter sinnvoll, um Lücken zu schließen. Denken Sie daran, dass es wichtig ist, [eine Sicherheits-Toolsuite](#) zu wählen, die sich in Microsoft integrieren lässt, um den Aufwand durch getrennte Tools zu minimieren.

MULTI-TENANT-MANAGEMENT MIT MEHREREN ANBIETERN

Ein Anbieter wie Hornetsecurity kann die Bereiche abdecken, die Microsoft offenlässt. So hat Microsoft beispielsweise jahrelang behauptet, dass eine Backup-Lösung für Microsoft 365 nicht erforderlich sei, bis Microsoft dann selbst eine eigene Lösung anbot. Auch wenn insgesamt immer weniger Lücken verbleiben, die Anbieter füllen können, wird eine immer bestehen bleiben: das Multi-Tenant-Management. Microsoft hat [Tenant Configuration Management APIs](#) veröffentlicht (zum Zeitpunkt der Erstellung dieses Berichts in der Preview-Phase), diese bieten jedoch derzeit keine MSP-gerechte Benutzeroberfläche. Für wirklich effizientes und umfassendes Multi-Tenant-Management bleibt ein Tool wie 365 Multi-Tenant Manager für MSPs unverzichtbar.



	USERS	GROUPS	POLICIES	SETTINGS	COMPLIANT
Tenant A	17	17	26	63	100%
Tenant B	15	12	30	46	100%
Tenant C	17	21	26	53	100%
Tenant D	10	25	27	39	100%
Tenant E					Not onboarded

Abbildung 16: Onboarding von Tenants in Hornetsecuritys 365 Multi-Tenant Manager für MSPs

Microsoft hat in einigen Produkten wie Defender XDR zwar Multi-Tenant-Funktionen ergänzt, diese aber mit Beschränkungen versehen, die aus Microsofts Enterprise-Perspektive erklärbar sind. So ist das Portal beispielsweise auf 100 Tenants begrenzt. Für größere MSPs ist das schnell zu wenig. In meinem siebenköpfigen MSP betreuten wir 80 Kunden und lagen damit nahe an dieser Grenze. Wer mit Blick auf Effizienz und gleichbleibende Servicequalität arbeitet, benötigt daher eine zusätzliche Lösung wie Hornetsecuritys 365 Multi-Tenant Manager für MSPs.

WEITERE ÜBERLEGUNGEN

Durch die vereinfachte Anbieterverwaltung gewinnen MSPs Zeit, sich auf die Bereitstellung höherwertiger Dienstleistungen zu konzentrieren, wie die Übernahme der Rolle eines virtuellen Chief Information Officer (CIO) oder Chief Information Security Officer (CISO). Dadurch können MSPs strategische Beratung leisten, Sicherheitsinitiativen an Geschäftszielen ausrichten und sich Wettbewerbsvorteile sichern. Kunden bewerten sichtbare Services höher, und konkrete Resultate wie eine verbesserte Sicherheitslage, die Einhaltung von Vorschriften und die Reduzierung von Risiken führen zu höherer Kundenzufriedenheit und -bindung. Durch die Konzentration auf strategische Dienstleistungen können MSPs nachhaltiges Geschäftswachstum erzielen und von Branchentrends profitieren, die höherwertige Dienstleistungen erfordern.

ZUSAMMENFASSUNG

Die Anbieterverwaltung in einem MSP erfordert eine sorgfältige Balance zwischen Effizienz und der Bereitstellung hochwertiger Lösungen. Die Entscheidung zwischen einem einzigen Anbieter und mehreren Best-of-Breed-Anbietern ist nicht einfach und erfordert die Berücksichtigung von Faktoren wie Verwaltungsaufwand, Kosten, Integration, Innovation und Anbieterabhängigkeit. Ein Single-Vendor-Ansatz vereinfacht die Verwaltung und kann Kosten sparen, birgt aber Abhängigkeiten und begrenzte Innovation. Best of Breed bietet Spezialisierung und Flexibilität, erhöht jedoch Komplexität und Kosten. Die richtige Wahl hängt letztlich von individuellen Zielen und Anforderungen des MSP und seiner Kunden ab. Ein durchdachter Entscheidungsprozess, zum Beispiel mithilfe einer Entscheidungstabelle oder einer SWOT-Analyse, kann dabei helfen, die beste Wahl zu treffen. Durch eine effiziente Verwaltung von Anbietern können sich MSPs darauf konzentrieren, hochwertigere Dienstleistungen bereitzustellen und nachhaltiges Geschäftswachstum zu erzielen.

Diese häufig übersehenen Elemente sind sowohl für Kunden als auch MSPs von großem Wert und verdeutlichen die Vorteile eines effizienten Managements von Anbieterbeziehungen.



KAPITEL 7: KI BEI IHREN KUNDEN, KI IN IHREM MSP

Generative KI und KI-Agenten verändern sowohl die internen Abläufe von MSPs als auch die ihrer Kunden. Das hohe Veränderungstempo erschwert es zusätzlich, als technischer Berater stets fundierte Orientierung zu geben. Dennoch gibt es einige grundlegende Schritte für den internen KI-Einsatz und die Unterstützung von Kunden bei deren KI-Implementierung, die jeder MSP beachten sollte, unabhängig davon, ob er aus zwei oder 25 Technikern besteht.

In diesem Kapitel betrachten wir Richtlinien zur akzeptablen Nutzung von KI (AI Acceptable Use Policies, AUP), Ethik, KI-Browser und KI-Governance. Außerdem beschäftigen wir uns mit Daten-Governance, Data Lifecycle Management (beides Bereiche, die traditionell nicht zum Kerngeschäft von MSPs gehören), Shadow AI sowie der Frage, wie sich diese Leistungen als Beratungs- und Serviceangebote für Kunden anbieten lassen.

Die KI-Revolution ist für MSPs eine Chance, ihr technisches Wissen unter Beweis zu stellen und zu den Wurzeln des MSP-Geschäfts zurückzukehren, nämlich als IT-Consultant zu agieren. Früher (in den 1990er Jahren) war die Einführung von Computern, Netzwerken und Servern in KMU komplex und erforderte viel Know-How. Dazu gehörte auch die Beratung des Kunden, um dessen Geschäftsprozesse zu verstehen und die richtige Technologie zu finden, um diese zu verbessern. Heute beschränken sich viele MSPs darauf, den laufenden Betrieb sicherzustellen. Doch die Implementierung von KI-Lösungen zur Automatisierung von Geschäftsprozessen erfordert das Verständnis dieser Prozesse und die Entwicklung maßgeschneiderter Lösungen – genau das ist IT Consulting. MSPs, die verstehen, dass es sich hierbei nicht um eine reine Tool-Einführung, sondern eine Governance-Entscheidung handelt, sind bestens aufgestellt, um ihren Kunden zum Erfolg mit KI zu verhelfen.

SHADOW AI

Die meisten Unternehmen nutzen bereits generative KI. Das reicht von wenigen Anwendern in KMU, die Berichte verfassen oder Marketingmaterial erstellen, bis hin zu vollständig automatisierten Workflows.

Der erste Schritt für den MSP sind Gespräche mit jedem Kunden, um dessen Verständnis von KI, den aktuellen Einsatz und die Erwartungen hinsichtlich dessen, was GenAI und Automatisierung für das Unternehmen leisten sollen, zu ermitteln. Der Geheimitipp vor diesen Gesprächen ist ein Werkzeug, das die tatsächliche Nutzung generativer KI im Unternehmen sichtbar macht: Shadow AI. Dies ist eine Anspielung auf den Begriff „Shadow IT“, bei der Einzelpersonen oder Teams Cloud-Dienste und -Tools nutzen, die nicht von dem Unternehmen genehmigt wurden, um ihre Arbeit zu erledigen. Die Nutzung dieser Tools führt zu Problemen wie mangelnde Kontrolle, fehlendes Monitoring und das Abfließen sensibler oder personenbezogener Daten außerhalb der Unternehmenskontrolle. Die gleichen Risiken bestehen auch bei Shadow AI (Shadow IT: Unbefugte könnten auf gemeinsam genutzte Daten zugreifen), jedoch sind es hier nicht nur theoretische Risiken, sondern reale: Jedes kostenlose Chatbot-Tool nutzt Prompts und hochgeladene Dokumente für Trainingszwecke seines Large Language Models (LLM). Das kann besonders bei personenbezogenen Daten problematisch sein. Auch kostenpflichtige LLM-Angebote mit Schutzmechanismen für Benutzerdaten erfordern genaue Prüfung. Die Verwaltung genehmigter und nicht genehmigter GenAI-Tools ist daher eine wichtige MSP-Aufgabe.

Es gibt mehrere Werkzeuge zur Erkennung von Shadow AI, darunter spezialisierte Lösungen wie Acuvity. Zusätzlich gibt es Funktionen in Microsoft, falls ein Drittanbieter keine Option ist. Ein Beispiel ist Defender for Cloud Apps, das entsprechende Dashboards enthält und in einigen Microsoft 365-Lizenzen enthalten ist, die MSPs bereits an ihre Kunden vertreiben.

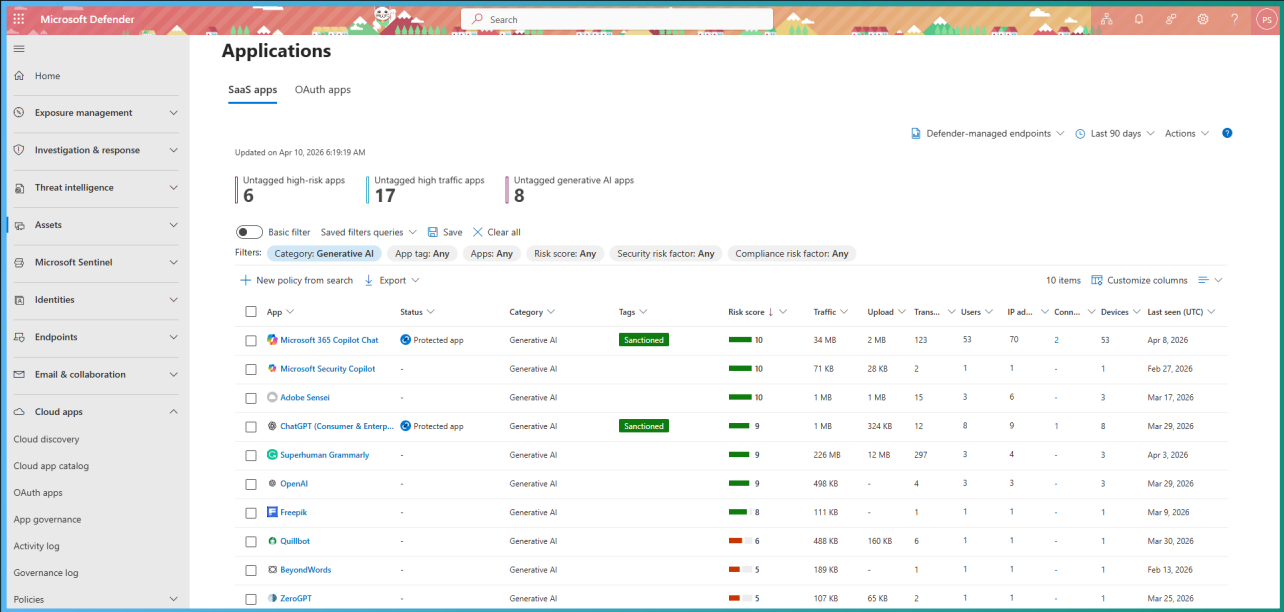


Abbildung 17: Erkennung von Shadow AI in Defender for Cloud Apps

Führen Sie diese Berichte aus und besprechen Sie die Ergebnisse mit dem Kunden. Meist zeigt sich klar, dass erwartete oder genehmigte GenAI-Anwendungen genutzt werden (M365 Copilot Chat und ChatGPT in Abbildung 2), daneben aber auch viele andere GenAI-Werkzeuge, darunter solche mit niedrigen Risikobewertungen.

RICHTLINIEN ZUR AKZEPTABLEN NUTZUNG VON KI

Dieses Gespräch führt schließlich dazu, dass für jeden Kunden regelmäßig Shadow-AI-Audits eingeführt werden und verdeutlicht die Notwendigkeit von Richtlinien zur akzeptablen Nutzung von KI. Dieses Dokument ist ein zentrales Instrument des Risikomanagements für Unternehmen. Es legt fest, welche KI-Werkzeuge verwendet werden dürfen und welche Daten damit geteilt werden dürfen. Eine grundlegende Richtlinie sollte Folgendes enthalten:

- » **Zweck der Richtlinie**
- » **Ethische Grundsätze**
- » **Verantwortlichkeiten der Mitarbeiter**
- » **Verbotene Nutzungszwecke**
- » **Durchsetzung der Richtlinie**

Verdeutlichen Sie, welche KI-Tools zulässig sind, und bieten Sie einen einfachen Weg für Mitarbeiter, neue Anwendungen zur Aufnahme in diese Liste vorzuschlagen.

Auch KI-Browser sind ein Bereich, der sich derzeit sehr schnell entwickelt. Mitarbeiter könnten sie installieren, um damit zu experimentieren oder sie mit Geschäftsdaten zu testen. Solche Browser sollten in der Richtlinie ausdrücklich behandelt werden. Viele davon sind noch sehr neu, bringen typische Anfangsschwachstellen mit und sind zudem für Prompt-Injection-Angriffe anfällig. Außerhalb strikt isolierter Netzwerke sind KI-Browser derzeit noch nicht für den geschäftlichen Einsatz geeignet und sollten blockiert werden.

Das gilt auch für den (zum Zeitpunkt der Erstellung dieses E-Books) neuesten KI-Hype, OpenClaw. Dieser KI-Agent kann viele autonome Aufgaben ausführen und Skills nutzen, um komplexe Aufgaben zu bewältigen, weist jedoch erhebliche Sicherheitslücken auf und gehört derzeit (noch) nicht in Unternehmensnetzwerke.

KI-GOVERNANCE

Der erfolgreiche Einsatz von KI-Automatisierung und agentischen Lösungen hängt nicht primär von der Wahl des richtigen LLMs, Chatbots oder Agenten ab. Die Herausforderung liegt darin, Geschäftsprozesse, Daten, Kontext und die Bereiche zu verstehen, in denen KI wirklich Mehrwert bringt.

Der Ausgangspunkt sind Daten. Sie müssen Ihren Kunden dabei helfen, Daten-Governance zu implementieren. Für viele KMU und MSPs bedeutet das lediglich, sicherzustellen, dass beispielsweise nur HR-Mitarbeiter Zugriff auf die HR-SharePoint-Site haben. Sobald Sie jedoch KI-Agenten einführen, benötigen diese Zugriff auf die richtigen Daten und den richtigen Kontext, um effektiv zu arbeiten. Gleichzeitig müssen Sie sicherstellen, dass sie keinen Zugriff auf Dokumente haben, die sie nicht einsehen sollten. Ebenso wichtig ist die Einführung von Data Lifecycle Management, sodass Daten nur so lange aufbewahrt werden, wie es erforderlich ist und automatisch archiviert werden, sobald sie nicht mehr benötigt werden. Wenn Copilot auf Vertragsdokumente aus 15 Jahren zugreifen kann, fällt die Ausgabe oft schlechter aus als bei einem aufgeräumten und zeitlich begrenzten Datenbestand.

Wenn Sie diese Vorarbeit mit Ihren Kunden nicht leisten, verstärkt eine KI-Einführung schlecht dokumentierte Abläufe und sorgt eher für Enttäuschung als für Effizienz.

In der Microsoft-Umgebung werden Data Security Posture Management (DSPM), Data Loss Prevention (DLP), Information Protection und Data Lifecycle Management unter Purview zusammengefasst (verfügbar in M365 E5 und als Add-on für M365 Business Premium). Sie können Dokumente manuell oder automatisch klassifizieren und dann Richtlinien festlegen, die die Freigabe von Dokumenten mit bestimmten Kennzeichnungen für Personen außerhalb des Kundenunternehmens verhindern oder deren Hochladen bzw. Verarbeiten durch KI-Tools unterbinden.

Hornetsecurity stellt mit [365 Permission Manager](#) eine besonders passende Lösung für die sichere Einführung von GenAI bereit. Es bietet einen klaren Überblick über Berechtigungen für jede SharePoint-Site, Teams und persönliche OneDrive for Business-Bereiche innerhalb des Tenants. Darüber hinaus ermöglicht es Ihnen die Zuweisung von Standard- oder benutzerdefinierten Vorlagen, um Berechtigungen und Freigaben zu steuern und überwacht riskante Änderungen kontinuierlich. Außerdem verwaltet es Freigabelinks effizient und vermittelt Ihnen ein klares Bild davon, wer was mit wem und für wie lange teilt. Gerade wenn Kunden Microsoft 365 Copilot nutzen, ist das Verständnis und die Governance von Dokumentzugriffen unverzichtbar. Andernfalls kann eine Anfrage wie „Wo finde ich Gehaltsinformationen?“ statt zu einem harmlosen Link auf allgemeine HR-Informationen direkt zu einer Tabelle mit den aktuellen Gehältern aller Mitarbeiter führen. Deshalb ist es wichtig, Kunden für diese Risiken zu sensibilisieren und mit 365 Permission Manager dafür zu sorgen, dass sie wirksam begrenzt werden.

Ein wesentlicher Bestandteil der Verwaltung von KI-Agenten besteht darin, sicherzustellen, dass ihre Identität eindeutig festgestellt wird und sie bei ihren Aktivitäten nachverfolgt werden können – eine Funktion, die in Entra unter „Agent ID“ hinzugefügt wurde.

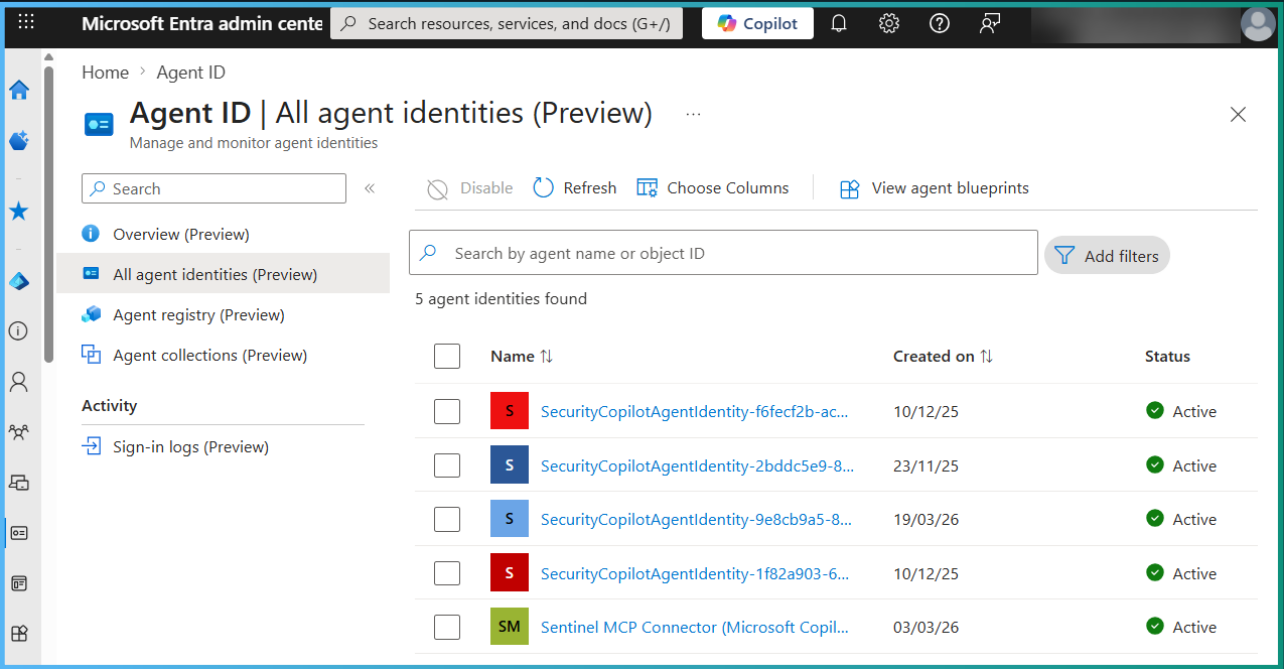


Abbildung 18: Agent ID in Entra

Im M365-Adminportal steht ein Agentenverzeichnis zur Verfügung. Dort können Sie Agenten blockieren, Microsoft- oder Drittanbieter-Agenten für alle Benutzer oder bestimmte Gruppen bereitstellen sowie Berechtigungen für Agenten vergeben, die Zugriff auf Daten benötigen.

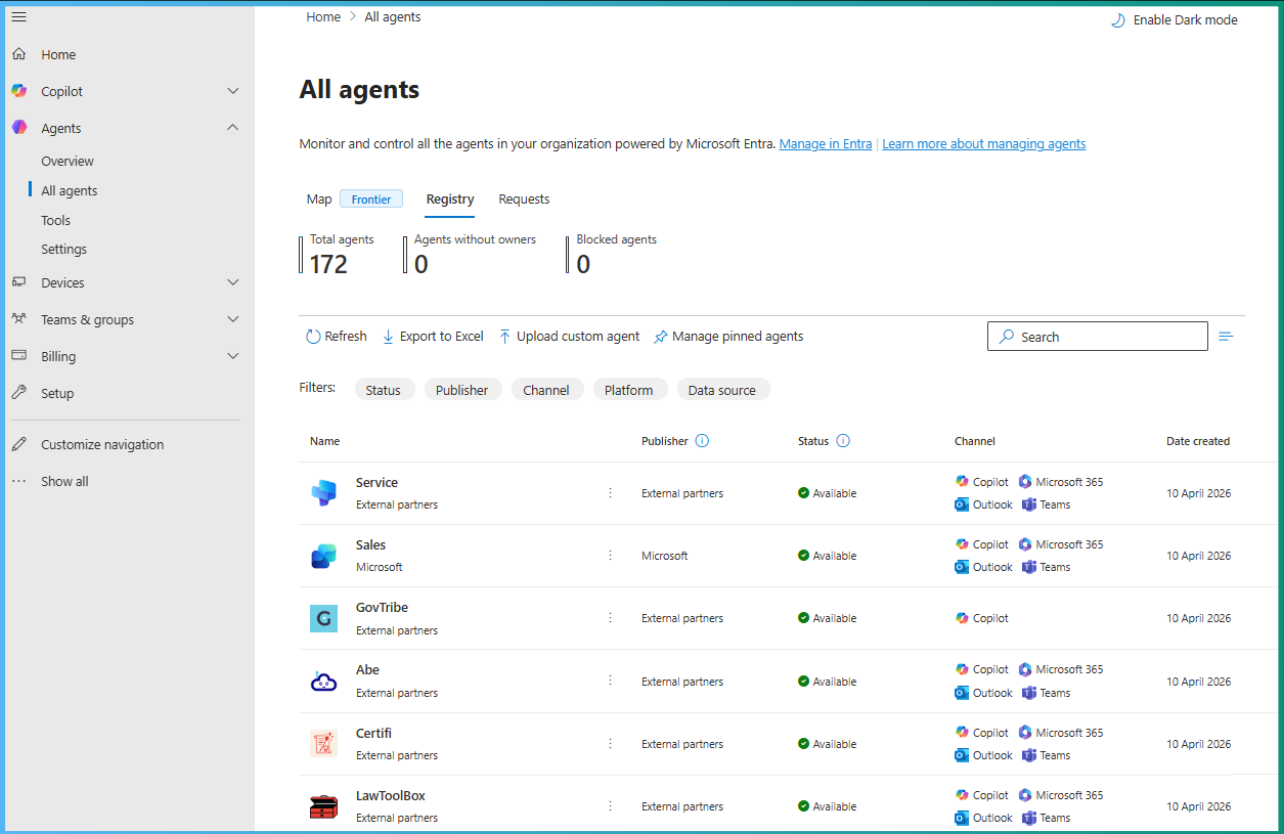


Abbildung 19: Agentenverzeichnis im M365-Adminportal

AI.MY ist ein praktischer AI Cyber Assistant von Hornetsecurity, der Benutzern und Kunden hilft, häufige Fehler zu vermeiden, indem er rechtzeitig auf Risiken hinweist. Gleichzeitig unterstützt er Techniker, wenn sie Unterstützung benötigen.

KI IST EINE CHANCE FÜR MSPS

Zu Beginn dieses Kapitels haben wir sowohl über den internen Einsatz von KI gesprochen, um die Effizienz in Ihrem MSP zu steigern, als auch darüber, Ihren Kunden dabei zu helfen, ähnliche Potenziale zu nutzen. Ein naheliegender Einstiegspunkt für einen MSP ist der Einsatz von KI-Agenten zur Bearbeitung häufiger und leicht automatisierbarer Supportanfragen. Hier sollten Sie langsam beginnen und sicherstellen, dass Änderungen von Menschen freigegeben werden. Governance bleibt auch hier zentral: Sie benötigen Audit- und Protokollierungssysteme, damit Sie jeden Schritt des Agenten nachvollziehen können. Weitere Effizienzpotenziale von KI-Automatisierung liegen in der Verarbeitung von Angebotsanfragen und der automatischen Erstellung erster Antwortentwürfe für Vertrieb und Technik.

Die oben beschriebenen Aufgaben sind größtenteils projektbasiert (mit Ausnahme der Überwachung von Shadow-AI-Nutzung und der Erstellung monatlicher Berichte) und eröffnen dem MSP so zusätzliche Einnahmequellen. Wer Kunden dabei unterstützt, KI erfolgreich einzuführen, muss jedoch weit mehr leisten als Technik einzuschalten. Es geht um das Verständnis bestehender Geschäftsprozesse, ihrer Lücken und des richtigen Zusammenspiels für Automatisierung. Hinzu kommt das Verständnis der Cybersicherheitsrisiken, die mit dieser sich rasch entwickelnden Technologie einhergehen, sowie die Frage, wie diese überwacht und verwaltet werden können.



KAPITEL 8: FAZIT

In diesem E-Book haben wir sechs wesentliche Faktoren behandelt, die einen effizienten MSP-Betrieb vorantreiben: Onboarding, Monitoring und Wartung, Kundenanpassung, Cybersicherheit, Anbieterverwaltung und GenAI. Für jeden Bereich haben wir Möglichkeiten zur Effizienzsteigerung beleuchtet und konkrete Wege aufgezeigt, um diese zu erreichen. Hier sind unsere Erkenntnisse.

EFFIZIENTES ONBOARDING

Um Effizienz beim Onboarding zu erreichen, müssen folgende vier Aufgaben erfüllt werden:

- » Automatisierung des Geräte-Onboardings
- » Automatisierung der Gerätekonfiguration
- » Standardisierung der Portalkonfiguration
- » Standardisierung der Sicherheitskontrollen

Der Einsatz integrierter und Drittanbieter-Tools zur Minimierung des Zeitaufwands für diese Aufgaben ist entscheidend, muss aber stets mit den Erwartungen des Kunden und einem guten Kundenerlebnis in Einklang gebracht werden. Dieses Gleichgewicht zu finden, wird sich langfristig auf die Kundenbeziehung auswirken. In unserer Diskussion haben wir die unterschiedlichen Sichtweisen von Kunden und MSPs herausgestellt. Diese Unterschiede existieren nicht nur in der Onboarding-Phase der Kundenbeziehung, sondern in jedem Aspekt.

MONITORING UND WARTUNG

Wir haben außerdem Aspekte der MSP-Effizienz bei Monitoring- und Überwachungsaktivitäten untersucht. Dabei haben wir uns eingehend mit den Vorteilen proaktiver Wartung, automatisierten Monitorings, klarer Incident-Response-Verfahren und belastbarer Disaster-Recovery-Planung befasst. In diesem Bereich besteht ein hoher Bedarf an Automatisierung, doch dabei darf die Kundenbeziehung nicht aus den Augen verloren werden.

MSPs haben, ähnlich wie beim Onboarding, die Möglichkeit, zu automatisieren und gleichzeitig den Kunden zu begeistern. Ein Großteil der Arbeit, die ein MSP routinemäßig leistet, ist für den Kunden unsichtbar. Ihre Helpdesk-Mitarbeiter sind somit Ihr Aushängeschild und ein entscheidender Faktor dafür, wie Ihre Kunden Ihre Dienstleistungen wahrnehmen. Freundlichkeit, Empathie und Effizienz sind daher der Schlüssel.

Durch die Umsetzung effektiver Verfahren und Pläne können MSPs ihre Leistung steigern, Stress reduzieren und eine höhere Rentabilität erzielen.

KUNDENANPASSUNG

Die Beherrschung von Anpassung und Änderungsmanagement ist für MSPs entscheidend, um sich im Markt zu differenzieren und Kunden einen Mehrwert zu bieten. Durch die Bereitstellung benutzerdefinierter Konfigurationen und standardisierter Vorlagen lassen sich individuelle Kundenanforderungen erfüllen und gleichzeitig betriebliche Effizienz sichern. Effektives Zeitmanagement, bei dem der Schwerpunkt auf der Anpassung statt auf der Bereitstellung liegt, ermöglicht es MSPs, den Großteil ihrer Zeit für kundenorientierte Aufgaben zu nutzen, was letztlich zu höherer Kundenzufriedenheit und einer stärkeren Marktpräsenz führt. Darüber hinaus ermöglicht dies dem MSP, sich auf bestimmte Branchen oder regulatorische Anforderungen zu spezialisieren und so die Effizienz und Rentabilität weiter zu steigern.

CYBERSICHERHEIT

Die Bedrohungslandschaft entwickelt sich ständig weiter. IT-Dienstleister, die sich auf KMU konzentrieren, müssen deshalb wachsam bleiben und einen proaktiven Ansatz in Bezug auf Cybersicherheit verfolgen. Mit den in Kapitel 4 beschriebenen Tools und Strategien lassen sich Kundennetzwerke und -Daten wirksam schützen, ohne Effizienz und Profitabilität aus dem Blick zu verlieren. Cybersicherheit ist ein kontinuierlicher Prozess und erfordert fortlaufendes Lernen und ständige Anpassung. Die dabei gewonnenen Erkenntnisse fließen dabei immer wieder in neue Standards und Vorgehensweisen ein. Dies erfordert, dass MSPs über entsprechend qualifizierte Mitarbeiter verfügen, die fachlich informiert, vorbereitet und handlungsfähig bleiben.

ANBIETERVERWALTUNG

Durch das hohe Tempo, mit dem sich das Marktumfeld verändert hat, ist bei vielen MSPs die Zahl der eingesetzten Anbieter im Laufe der Zeit stark gewachsen. Oft wurden zusätzliche Hersteller und Lösungen eingeführt, um mit neuen Anforderungen Schritt zu halten. Diese Entscheidungen unter Effizienzgesichtspunkten erneut zu bewerten, ist daher eine wichtige Aufgabe. Als Hilfsmittel dafür wurden in Kapitel 5 zwei Ansätze vorgestellt: die Vergleichstabelle und die SWOT-Analyse.

Vereinfachte Anbieterverwaltung schafft Freiräume, damit sich MSPs stärker auf höherwertige Leistungen konzentrieren können, wie virtuelle CIO- oder CISO-Services. Dadurch können MSPs ihre Kunden strategischer beraten, Cybersicherheitsmaßnahmen besser an Geschäftsziele ausrichten und sich klarer im Wettbewerb positionieren. Kunden messen sichtbaren Leistungen oft einen besonders hohen Wert bei, sodass sich konkrete Ergebnisse wie eine verbesserte Sicherheitslage, die Einhaltung regulatorischer Anforderungen und reduzierte Risiken direkt auf die Kundenzufriedenheit und -bindung auswirken. Wer sich als MSP in Richtung strategischer und sicherheitsnaher Leistungen weiterentwickelt, schafft die Grundlage für höhere Margen, zusätzliche Umsatzquellen und langfristig wertvollere Kundenbeziehungen. Mit einem stärkeren Fokus auf strategische Services können MSPs nachhaltiges Geschäftswachstum erzielen und von Markttrends profitieren, die genau solche Leistungen zunehmend nachfragen.

GENERATIVE KI

Dieser Bereich hat das größte Potenzial, die Geschäftswelt im Allgemeinen und das MSP-Modell im Besonderen grundlegend zu verändern. GenAI bietet enorme Chancen für Effizienz und Automatisierung, muss aber sorgfältig gesteuert werden. Für MSPs entstehen hier neue Kompetenzfelder wie Daten-Governance (was deutlich über Backup und das Setzen von SharePoint-Berechtigungen hinausgeht), Data Lifecycle Management, Shadow-AI-Monitoring sowie ein fundiertes Verständnis von Geschäftsprozessen und der Frage, an welchen Stellen KI den größten Nutzen stiften kann.

SCHLUSSWORT

Wenn Inhaber und technische Mitarbeiter eines MSP die sechs in diesem E-Book behandelten Bereiche beherrschen, sind die Voraussetzungen für nachhaltigen Erfolg gegeben. MSPs spielen für den Erfolg von Unternehmen jeder Größe und in jeder Volkswirtschaft eine zentrale Rolle. Nur wenige Unternehmen sind groß genug, um intern eine eigene IT-Abteilung mit der Breite an Fähigkeiten aufzubauen, die ein guter MSP bietet. Das Marktpotenzial für einen effizienten MSP ist daher enorm und die Chancen sind nahezu unbegrenzt. Wenn ein MSP erfolgreich ist, profitieren alle. Effizienz ist dabei ein entscheidender Faktor für diesen Erfolg.

ÜBER DEN AUTOR

Paul Schnackenburg

Paul Schnackenburg begann seine IT-Karriere, als DOS und 286-Prozessoren noch die neuesten Technologien waren. Heute leitet er Expert IT Solutions, einen MSP an der Sunshine Coast in Australien.

Als angesehener Technologieautor ist Paul in der Community aktiv und schreibt ausführliche Fachartikel mit den Schwerpunkten Cybersicherheit, Microsoft 365 und damit verbundenen Cloud-Diensten.

Er verfügt über MCSE-, MCSA- und MCT-Zertifizierungen.

