Februar 2024

ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

Hilfsmittel für Einstieg und Arbeiten mit der BSI-IT-Grundschutz-Methodik

von Oliver Flüs

Die BSI-Grundschutz-Methodik ist eine methodische Arbeitsbasis für Aufbau und Pflege von Informationssicherheit. Verschiedene Hilfsmittel sind über BSI-Webseiten zugänglich, man muss allerdings wissen, wo, wozu, von wem, usw.

Seite 9

Was ist wichtiger: weniger Komplexität oder mehr Diversität?

von Dr. Behrooz Moayeri

In der letzten Insider-Ausgabe des Jahres 2023 bin ich auf die wichtigsten Netztrends in 2024 eingegangen. Ich habe darauf hingewiesen, dass die Ausfallsicherheit von Netzen fast immer mit redundanter Hardware in Verbindung gebracht wird.

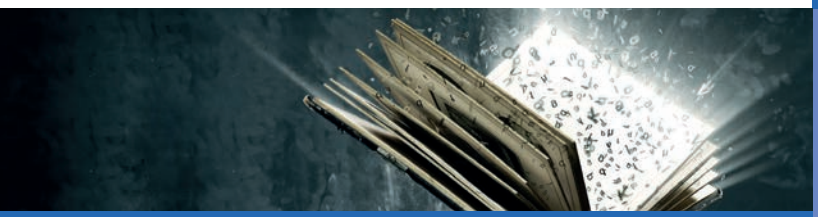
Seite 2

Sicherheitsmaßnahmen für Microsoft-365-Umgebungen

von Aaron Siller

Die Wahrung der Sicherheit von Unternehmensdaten und -infrastrukturen ist unverzichtbar. Microsoft 365, eine umfassende Suite von Produktivitätstools und Cloud-Diensten, spielt bei vielen Unternehmen eine tragende Rolle, werden doch viele Bestandteile der Suite mehr oder weniger intensiv genutzt.

Seite 28



Webinar der Woche

Schluss mit Fachchinesisch – endlich verstehen mich die anderen

Seite 26

Wird Wi-Fi 7 der 5G-Killer?

von Dr. Joachim Wetzlar

Es ist so weit: Am 8. Januar hat die Wi-Fi Alliance ihr Zertifizierungsprogramm Wi-Fi CERTIFIED 7™ vorgestellt [1]. Sie kennen die Vorgehensweise bereits von früheren WLAN-Versionen: Der Standard ist seitens des IEEE noch lange nicht verabschiedet, Hersteller und Ausrüster einigen sich aber schon einmal auf die wesentlichen Details, um ihre Produkte einigermaßen investitionssicher vermarkten zu können.

Seite 24

Was ist wichtiger: weniger Komplexität oder mehr Diversität?

von Dr. Behrooz Moayeri

In der letzten Insider-Ausgabe des Jahres 2023 bin ich auf die wichtigsten Netztrends in 2024 eingegangen. Ich habe darauf hingewiesen, dass die Ausfallsicherheit von Netzen fast immer mit redundanter Hardware in Verbindung gebracht wird. Es folgte die Warnung vor Ausfallszenarien, zu denen es trotz einer durchgängigen Hardware-Redundanz kommt. Aus Erfahrung merkte ich an, dass Software auf Netzkomponenten zum Single Point of Failure werden kann, wenn alle Geräte mit derselben fehlerhaften Software arbeiten. Ferner erwähnte ich die durchaus bewährte Robustheit des Internets, das unter anderem zwecks Ausfallsicherheit verschiedene administrativen Domänen (Autonome Systemen, AS) umfasst.

Nun ist ein Unternehmensnetz per se EINE administrative Domäne. Für das Netz eines Unternehmens ist in der Regel eine organisatorische Einheit zuständig. Große Unternehmen delegieren schon mal den Betrieb von Teilbereichen ihrer Netze an lokale Einheiten oder spezialisierte Teams, die sich zum Beispiel um das RZ-Netz kümmern. Es gilt jedoch fast immer, dass für eine bestimmte Netzfunktion eine organisatorische Einheit zuständig ist. Zum Beispiel trägt das WAN-Team die Verantwortung dafür, dass verschiedene Standorte des Unternehmens miteinander kommunizieren können, unabhängig davon, wie die lokalen Netze an den Standorten aussehen und wie und von wem sie betrieben werden.

Insofern kann eine ganz wichtige Funktion, auf die das gesamte Unternehmen angewiesen ist, ausfallen, weil ein Team oder sogar eine einzelne Person einen Fehler gemacht hat. Davor sind nicht einmal große Hyperscaler wie Microsoft gefeit, wie einige Vorfälle in der jungen Vergangenheit gezeigt haben.

Software von Netzkomponenten als Fehlerquelle

Netzadministratoren sind nicht die einzigen Menschen, denen Fehler unterlaufen können. Auch die Entwickler von Software auf Netzkomponenten sind Menschen und können Software-Bugs produzieren. Zu Netzkomponenten zähle ich in diesem Zusammenhang nicht nur Switches und Router, sondern auch Firewalls. Eine der etablierten Antworten der Unternehmen auf zunehmende Cyber-Risiken ist die Segmentierung von Netzen mittels Firewalls. Angesichts der Wichtigkeit mancher segmentübergreifender Kommunikation, zum Beispiel Zugriff der Clients im Campusnetz auf Server im RZ-Netz, werden zum Beispiel Data Center Firewalls redundant ausgelegt. Das gängigste Modell dafür ist ein Cluster von zwei Firewall-Knoten desselben Herstellers, auf denen dieselbe Software läuft. Weist diese Software ein Problem auf, kann sie ausfallen, und mit ihr sämtliche Client-Server-Zugriffe.

Sollte man deshalb grundsätzlich für alle kritischen Funktionen mindestens zwei Produkte einsetzen, die von möglichst keiner einzelnen Fehlerquelle betroffen sein können? Ist es praktikabel, zum Beispiel ein RZ-Netz über Firewalls von zwei verschiedenen Herstellern mit dem Campusnetz zu verbinden? Die Antwort auf diese Frage ist nicht trivial. Die für eine IT verantwortlichen Personen sollten sich der Frage stellen, was wichtiger ist: weniger

Hilfsmittel für Einstieg und Arbeiten mit der BSI-IT-Grundschutz-Methodik

von Oliver Flüs

Die BSI-Grundschutz-Methodik ist eine methodische Arbeitsbasis für Aufbau und Pflege von Informationssicherheit. Verschiedene Hilfsmittel sind über BSI-Webseiten zugänglich, man muss allerdings wissen, wo, wozu, von wem, usw.

Sie können den Einstieg erleichtern und Fortgeschrittenen helfen, neue Themen zu beherrschen. Voraussetzung für den erfolgreichen Einsatz solcher Vorlagen und Hilfen zur Selbsthilfe: „Gewusst, wo“, aufmerksames Lesen und Mut zur eigenen Entscheidung – also Mitdenken! Hierzu soll dieser Artikel einführen, das Auffinden erleichtern und Tipps aus Praxiserfahrung geben.

Informationssicherheit: wichtig, doch nicht einfach

Informationssicherheit ist ein wichtiges Thema in jeder Umgebung. Das gilt für Unternehmen genauso wie für Behörden, für kleine Umgebungen wie „Small Offices“, Handwerksbetriebe und kleine Geschäfte ebenso wie für große Büro- oder Produktionsstandorte. Ohne Informationen und deren Nutzung mittels Informationstechnik kommt praktisch niemand mehr aus. Sind Informationen nicht zugänglich oder unbrauchbar, stört dies die auf diese Informationen angewiesenen Arbeitsabläufe und Tätigkeiten. Je nach Umfang kann dies bis zum völligen Stillstand aller Prozesse und Aktivitäten führen. Je länger ein solcher Zustand andauert, umso schädlicher sind die Folgen. Kleinere Störungen und Ausfälle hat jeder schon in seiner Arbeitsumgebung erlebt. Von schlimmeren Vorfällen kann man mindestens in der Presse lesen, etwa wenn davon berichtet wird, dass irgendwo per Verschlüsselungs-Schadsoftware Datenbestände unbrauchbar gemacht worden sind. Fallen Informationen in unbefugte Hände, kann dies ebenfalls schweren Schaden anrichten. Wettbewerbsvorteile können verloren gehen, Strafen und Auftragsverluste wegen Verletzung vertraglicher Vertraulichkeitsvereinbarungen drohen. Selbst ohne konkreten Vorfall dieser Art kann eine empfindliche Strafe verhängt werden, wenn den Anforderungen an angemessenen Schutz von personenbezogenen Daten nicht entsprochen wird.

„Plug and play“, „out of the box“ oder ganz modern „in der Cloud“ sind Begriffe, die suggerieren, dass man sich darauf konzentrieren kann, Lösungen geschickt und erfolgreich zu nutzen. Dieses Versprechen mag bedingt in dem Sinne gelten, dass sich längst nicht jeder mit IT-Lösungen so auskennen muss, dass es zum Do-it-yourself-Betrieb oder auch nur zur Feineinrichtung wie für die eigenen Nutzungsfälle reicht. Für den Umgang mit Informationssicherheitsrisiken funktioniert dieses Prinzip des möglichst umfassenden Delegierens jedoch nicht!

Digitalisierung ist als Ziel und Notwendigkeit praktisch überall gesetzt. Die Möglichkeiten, wo und wie Informationen und Informationstechnik (IT) als Arbeitsgrundlage genutzt werden können und mit der Zeit unentbehrlich werden, nehmen ständig zu. Damit ver-

Sicherer Betrieb von Container-Technologien

Mit Dr. Markus Ermes sprach Christiane Zweipfennig

Container-Technologien als schnelle, ressourcenschonende und flexible Verteilung von Software gewinnen für moderne Anwendungen und Rechenzentren zunehmend an Bedeutung. Unternehmen, die Container-Technologien für die Entwicklung und den Betrieb von Software einsetzen, sollten Sicherheitsaspekte bereits vor der Einführung beachten. Dies setzt eine gute Planung voraus. Zusätzlich muss die Sicherheit während des gesamten Lebenszyklus der Container aufrechterhalten und verbessert werden. Dazu ist es erforderlich, dass alle Beteiligten wissen, welche Anforderungen zu beachten sind und über das entsprechende Know-how verfügen, diese auch umsetzen zu können.

Dr. Markus Ermes ist studierter Physiker und hat im Bereich der optischen Simulation seine Doktorarbeit geschrieben. Im Rahmen seiner Promotion hatte er schon immer viele Berührungspunkte mit der IT. So war er an der RWTH Aachen und in seinem Job am Forschungszentrum Jülich auch im Bereich der System- und Netzwerkadministration tätig. Seine Affinität zur IT veranlasste ihn vor knapp sieben Jahren dazu, zu ComConsult zu wechseln.

Markus, was sind deine Aufgaben bei ComConsult?

Ursprünglich war ich bei ComConsult im Competence Center Cloud und Data Center für die Themenbereiche Virtualisierung, Storage, Backup und Rechenzentrumsnetze zuständig. Mittlerweile beschäftige ich mich darüber hinaus viel mit der IT-Sicherheit, die im Rechenzentrumsbereich ebenfalls eine entscheidende Rolle spielt. Auch im Bereich Netze sind die Übergänge fließend.

Container-Technologien sind aktuell ein großes Thema. Warum?

> Software einfach installieren und laufen lassen

Vor mehr als einem Jahrzehnt hat das Thema Container mit Docker weltweit an Fahrt aufgenommen. Entwickler haben damit die Chance erhalten, dass alles, was für das Entwickeln des Programms notwendig war, mitgeliefert wurde. Es war nicht mehr nötig, eine Vorlage für eine virtuelle Maschine mit Betriebssystem und allem, was dazugehört, bereitzustellen. Mit anderen Worten: Software konnte man jetzt schlank in einer Form verpacken, die es ermöglichte, sie einfach zu installieren und laufen zu lassen. Inzwischen stellen viele Softwareentwickler ihre Software nur noch in dieser Form bereit. Kunden, die ich im Rechenzentrumsbereich berate, setzen sich stellenweise unter Zähneknirschen mit dem Thema auseinander, weil sie ihre Software nur noch in dieser Form erhalten. Technisch gesehen sind Container-Technologien eine interessante Sache: Sie sind schlank, einfach zu handhaben und lassen sich sehr gut automatisieren.

Die Hersteller von Kubernetes sind momentan sehr aktiv. Weshalb?

Container in ihrer ursprünglichen Form laufen auf einer einzelnen Maschine. Wenn diese Maschine ausfällt, fallen auch die An-

Wird Wi-Fi 7 der 5G-Killer?

von Dr. Joachim Wetzlar

Es ist so weit: Am 8. Januar hat die Wi-Fi Alliance ihr Zertifizierungsprogramm Wi-Fi CERTIFIED 7™ vorgestellt [1]. Sie kennen die Vorgehensweise bereits von früheren WLAN-Versionen: Der Standard ist seitens des IEEE noch lange nicht verabschiedet, Hersteller und Ausrüster einigen sich aber schon einmal auf die wesentlichen Details, um ihre Produkte einigermaßen investitionssicher vermarkten zu können. Immerhin rechnet man bei IEEE mit einer Verabschiedung des zugrundeliegenden Standards IEEE 802.11be noch in diesem Jahr [2]. Die Task Group 11be hat im Dezember 2023 die erforderliche Zustimmung zu ihrem Draft 5.0 erhalten. Jetzt ist als nächsthöheres Gremium die IEEE Standards Association dran.

Nach “Very High Throughput” (Wi-Fi 5) und “High Efficiency WLAN” (Wi-Fi 6) kommt mit Wi-fi 7 nun “Extremely High Throughput” (EHT). Wer hätte das gedacht: Abermals höherer Durchsatz mit WLAN. Und so sind einige der gewählten Konzepte naheliegend. Mein Kollege Dr. Johannes Dams wusste das im Grunde bereits vorletztes Jahr zu berichten [3]. Fangen wir mit den nahliegenden Lösungen an:

- 320 MHz Kanalbandbreite: Doppelte Bandbreite ergibt doppelten Durchsatz. Das Konzept kennen wir bereits seit mehr denn 10 Jahren. Es wurde mit IEEE 802.11n das erste Mal angewandt. Nur: zum einen bedeutet doppelte Bandbreite auch doppelte Sendeleistung. Und da das in der Regel nicht erlaubt ist, doppeltes Rauschen beim Empfänger. Man muss also näher heran an den Access Point (AP). Zum zweiten haben wir in Europa eh nicht genügend Frequenzen, um auf dieser Basis eine sinnvolle Kanalplanung durchführen zu können. Das taugt also allenfalls für die Wohnzimmerecke.

- 4096 QAM: Die Quadraturamplitudenmodulation wurde noch einmal aufgebohrt. Pro Zeiteinheit lassen sich somit 20% mehr Daten übertragen als noch mit Wi-Fi 6, das „nur“ bis zu 1024 QAM unterstützte. Auch dafür braucht es eine hohe Signalstärke am Empfangsort. Die Praktiker wissen, dass in WLANs üblicher AP-Dichte meist nicht mehr als die Hälfte dessen erreicht wird. Oder anders ausgedrückt: Damit hoher Durchsatz auch außerhalb des Wohnzimmers möglich wird, braucht es wesentlich mehr APs als Sie und wir derzeit installiert haben.

- 512 Compressed Block Ack: Bis zu 512 Pakete (MAC Protocol Data Units, MPDUs) lassen sich auf einmal senden und mit einem einzigen Paket quittieren. Dadurch spart man einen Haufen Wartezeit, Präambel und Header ein. Der Performance-Gewinn ist erheblich, wenn eine Station viele Daten zu versenden hat. Die Idee ist aber schon alt; Wi-Fi 6 unterstützte 256 Compressed Block Ack.

- Multiple RUs to a single STA (M-RU): Das Konzept der Resource Units stammt bekanntlich aus Wi-Fi 6. Mehrere Stationen können gleichzeitig adressiert werden, indem man ihnen verschiedene Unterträger der OFDM zuweist. Die Unterträger wurden in Resource Units (RUs) gruppiert. Einer Station wird in Wi-Fi 6 immer genau eine RU vom AP zugewiesen. Das Verfahren ist auch unter der Bezeichnung Orthogonal Frequency Division Multiple Access (OFDMA) bekannt und stammt letztlich aus dem Mobilfunk. Dort ist es, was die Zuweisung von RUs angeht, flexibler als im WLAN. M-RU schwächt diesen Nachteil ab, indem es erlaubt, einer Station mehrere RUs flexibel zuzuweisen.

Daneben gibt es jedoch wirklich neue Features in Wi-Fi 7. Sie werden vor allem damit beworben, dass zukünftig Anwendungen aus Industrie und Augmented / Virtual Reality bis hin zu Notruffähigkeit auf Basis von WLAN möglich werden sollen. Sie erinnern sich, das war auch eine wesentliche Werbeaussage bei der Einführung des 5G-Mobilfunks. Ich nenne zwei interessante neue Features von Wi-Fi 7:

Sicherheitsmaßnahmen für Microsoft-365-Umgebungen

von Aaron Siller

Die Palette von Diensten in Microsoft 365, darunter Exchange Online, SharePoint, OneDrive und Microsoft Teams, erfordert spezifische Sicherheitsvorkehrungen, um Gefahren wie Phishing, Datenlecks und unbefugtem Zugriff wirkungsvoll entgegenzutreten. Der Prozess der Sicherheitshärtung sollte sämtliche Facetten der Umgebung umfassen, angefangen bei der Konfiguration und sicherheitstechnischen Optimierung der Dienste bis hin zur Überwachung sämtlicher Aktivitäten. Im nachfolgenden Artikel werden bewährte Methoden sowie technische Ansätze präsentiert, um die Sicherheit von Microsoft-365-Umgebungen effizient zu maximieren.

Effektives Identitäts- und Zugriffsmanagement in der IT-Sicherheit

Das Management von Identitäten und Zugriffen ist ein entscheidender Faktor in einer gesicherten Microsoft-365-Umgebung. Nachfolgend einige bewährte Praktiken zum Identity and Access Management (IAM):

1. **Mehrstufige Authentifizierung (MFA)**: Die Integration von MFA stellt einen grundlegenden Schutzmechanismus dar. In Kombination mit Benutzernamen und Passwort wird eine zusätzliche Sicherheitsebene geschaffen, indem ein weiterer Authentifizierungsfaktor erforderlich ist. Besondere Aufmerksamkeit sollte darauf liegen, MFA-Methoden zu nutzen, die gegen Phishing resistent sind, während unsichere Varianten wie SMS oder Telefonanrufe vermieden werden.

2. **Optimierung des Lebenszyklusmanagements von Identitäten:** Ein effizientes Management des gesamten Lebenszyklus von Benutzeridentitäten ist entscheidend. Die Automatisierung von Prozessen wie der Erstellung, Änderung und Deaktivierung von Benutzerkonten gewährleistet, dass nur autorisierte Personen Zugriff haben. Regelmäßige Überprüfungen sind erforderlich, um veraltete oder nicht mehr benötigte Konten zu identifizieren und zu deaktivieren.

3. **Implementierung von Zugriffskontrollen und Just-in-Time-Zugriff:** Klare Richtlinien für den Zugriff auf Ressourcen und Daten sind von großer Bedeutung. Die Nutzung von rollenbasierter Zugriffssteuerung (RBAC) hilft sicherzustellen, dass Benutzer nur die Berechtigungen erhalten, die für ihre jeweilige Rolle erforderlich sind. Regelmäßige Überprüfungen und Aktualisierungen der Zugriffsrechte sind entscheidend, um sicherzustellen, dass sie den aktuellen Anforderungen entsprechen. Die Verwendung des Privileged Identity Management ist dabei empfehlenswert, um einen Just-in-Time Zugriff einzurichten und damit limitierte sowie globale Administratoren weiter zu schützen. Viele Unternehmen setzen nämlich zumeist auf eine einzige Administratorrolle, die zudem noch 24/7 zugänglich ist.

4. **Monitoring und Benachrichtigungen Einrichten:** Die Implementierung eines umfassenden Überwachungssystems für Benutzeraktivitäten ist entscheidend. Durch die Einrichtung von Alarmen für ungewöhnliche Aktivitäten oder verdächtige Anmeldeversuche können potenzielle Sicherheitsverletzungen frühzeitig erkannt und entsprechend darauf reagiert werden. Die Nutzung von Entra ID Identity Protection und der Auditierung im Purview Compliance-Portal kann in diesem Kontext äußerst hilfreich sein.