NAC auf dem Stand der Technik

Einsatzmöglichkeiten von Netzwerkzugangskontrolle im Rahmen der Datenschutzgrundverordnung (DSGVO)

Der kontrollierte Netzwerkzugang ist die erste Verteidigungslinie vor unberechtigten Zugriffen von außen auf sensible Unternehmens- und Kundendaten

Laut IDC [1] und Nifis [2] war noch vor etwa einem halben Jahr ein Großteil der deutschen Unternehmen nicht, oder nicht ausreichend auf die kommende Datenschutzgrundverordnung (DSGVO) vorbereitet. Mittlerweile haben jedoch viele tüchtig aufgeholt und gute Fortschritte auf dem Weg zur DSGVO-Konformität gemacht. Dennoch bleibt es eine sehr komplexe Angelegenheit. Unternehmen müssen ein ganzes Paket an Sicherheitsaspekten beachten und umsetzen. Zudem müssen die dazu eingesetzten Lösungen

Autor: Christian Bücker, Geschäftsführer macmon secure GmbH

dem „Stand der Technik“ entsprechen und effizient ineinander greifen, damit die geforderten technischen und organisatorischen Maßnahmen korrekt abgebildet werden.

Neben den internen Prozessen in der Datenverarbeitung und Kundenansprache, die durch die DSGVO runderneuert werden müssen, ist die Absicherung sensibler, personenbezogener Informationen im Unternehmen ein wichtiger Punkt. Neben den drohenden Bußgeldern bei Nichteinhaltung der Vorgaben der Verordnung, stellt die Benachrichtigungspflicht bei kritischen Datenpannen eine weitere ernstzunehmende Konsequenz für Unternehmen dar. Dadurch drohen enorme Reputationsschäden und damit handfeste Einbußen bei der Profitabilität. Solche Datenpannen im Vorfeld zu verhindern, ist also wichtiger denn je.

Der kontrollierte Netzwerkzugang ist in diesem Zusammenhang die erste Verteidigungslinie vor unberechtigten Zugriffen von außen auf sensible Unternehmens- und Kundendaten. Damit bildet Netzwerkzugangskontrolle (Network Access Control, NAC) einen der wichtigsten Pfeiler in der DSGVO-Strategie eines jeden Unternehmens.

Lückenlose Absicherung, Überprüfung und Dokumentation

macmon NAC (https://www.macmon.eu/), die führende deutsche Lösung für Netzwerkzugangskontrolle, bietet die Möglichkeit, zahlreiche Anforderungen der DSGVO effektiv zu unterstützen.

Die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierte Lösung macht aus heterogenen und komplexen Netzwerken eine intelligente Einheit, und ermöglicht bei minimalem Aufwand die effiziente Überwachung und den Schutz vor unbefugten Zugriffen. So gewährleistet macmon beispielsweise eine eindeutige Übersicht und Dokumentation des lokalen Netzwerkes und dessen Zugänge. Außerdem protokolliert es lückenlos alle Zugangsversuche und erkennt auch, wenn ein solcher zu einer ungewöhnlichen Uhrzeit stattfindet.

Um den Zugriff auf sensible Netzwerkbereiche vollkommen zu trennen, sollte das Netzwerk segmentiert werden. In macmon erfolgt die Segmentierung in Verbindung mit einfach zu administrierenden Endgerätegruppen. Dadurch wird das Ausmaß der Geräte, die für die gesicherte Verarbeitung besonders schützenswerter Daten beachtet werden müssen, erheblich reduziert und gleichzeitig auf die entscheidenden Geräte fokussiert. Eine übersichtliche Weboberfläche bietet dazu einen Überblick, welche Geräte eine Verbindung erhalten können, und aktuell erhalten. Endgeräte, die nicht DSGVO-konform sind, weil sie den Sicherheitsanforderungen nicht, oder nicht mehr entsprechen, isoliert macmon von sensiblen Bereichen und verschiebt sie in die Quarantäne. Das reduziert die Arbeitsbelastung von IT-Administratoren erheblich und ermöglicht die Einhaltung von in der DSGVO geforderten Prozessen auf technischer und organisatorischer Ebene. Ne-

[1] http://idc.de/de/ueber-idc/press-center/65095-idc-studie-zur-eu-datenschutz-grundverordnung-44-prozent-der-unternehmen-in-deutschland-sind-noch-nicht-ausreichend-vorbereitet

[2] http://www.nifis.de/veroeffentlichungen/news/article/studie-dsgvo/

ben der Alarmierung und der Verhinderung von unerwünschten Netzwerkzugriffen, stellt die dynamische Segmentierung von Netzwerken in Virtual Local Area Networks (VLANs) den effektivsten und sichersten Weg dar, um unbefugten Zugriff auf Daten zu verhindern. Die Haltung der sensiblen Daten auf separaten Servern - um diese nur innerhalb definierter Netzwerksegmente erreichbar zu machen - sorgt in Verbindung mit macmon Network Access Control für größtmöglichen Schutz.

Neben der Netzwerkzugangskontrolle wird auch die detaillierte Überprüfung der zugelassenen Systeme auf Einhaltung der Sicherheitsrichtlinien immer wichtiger. Eine permanente Überprüfung des „Compliance-Status“ und die automatisierte Durchsetzung der Vorgaben sind damit unumgänglich. Mit der macmon Compliance (https://www.macmon.eu/compliance/) erhalten Anwender die Option, mehrere, verknüpfbare Komponenten zu nutzen, um die Unternehmensrichtlinien effektiv durchzusetzen. Wichtig zu wissen ist dabei, dass 99 Prozent der Unternehmen bereits Systeme im Einsatz haben, die in der Lage sind, den Compliance-Status der Endgeräte zu ermitteln und die Administratoren über Abweichungen zu informieren. Fast alle haben jedoch gemein, dass die effektive Durchsetzung der Richtlinien in der Regel von Hand oder zumindest reaktiv erfolgen muss.

Genau hier bietet macmon die entscheidende Unterstützung. Je nach Anforderung kann der Compliance-Status von externen Quellen empfangen, oder durch die Anbindung fremder Datenbanken aktiv eingeholt werden. Innerhalb der macmon-GUI wird zu jedem Endgerät der Compliance-Status angezeigt. Wird dieser durch ein anderes System, wie beispielsweise Endpoint Security, Intrusion Prevention, Security Incident and Event Management, Patch Management oder Schwachstellen-Management verändert, so wird die Änderung, einschließlich der Angabe der Quelle und des Grundes, ebenfalls angezeigt. Das flexible macmon-Regelwerk erlaubt dann, auf gewohnt einfache Weise, eine Konfiguration der Reaktion auf die Status-Änderung. Endgeräte, die nicht mehr compliant sind, werden dann beispielsweise automatisch in Quarantäne, und nach erfolgter Heilung und entsprechend erneuter Status-Veränderung, wieder in ihren ursprünglichen Netzwerkbereich verschoben. Über die Report- und die Statistik-Funktionen bietet die macmon Compliance eine umfassende Übersicht über den Sicherheitszustand, die übermittelnden Quellen zum Compliance-Status und Informationen zu Sicherheitsabweichungen der verwalteten Endgeräte.

Maximaler Mehrwert durch 100-prozentige Nutzung bestehender Infrastrukturen

Die Kombinationsmöglichkeiten mit weiteren Technologieanbietern erlauben es, macmon als zentrale Kraft im Netzwerk zu nutzen. Gerade die völlige Herstellerunabhängigkeit sorgt an dieser Stelle dafür, dass bereits getätigte Investitionen durch macmon noch mal an Wert gewinnen. Vorhandene Systeme, mit der Funktion der Richtlinienüberprüfung, erhalten durch macmon eine automatisiert durchsetzende Instanz. Ein entscheidender Vorteil der Kombination verschiedener Lösungen ist dabei, dass die Zuständigkeiten der einzelnen IT-Bereiche nicht verändert werden. Wie und wann auf einen Richtlinienverstoß reagiert wird, entscheidet der Administrator des jeweiligen Systems. Die Netzwerkabteilung bietet mit macmon einen Automatismus zur Erfüllung von Isolationsaufgaben an. Sie muss in keiner Weise selber eingreifen, da die Isolierung und das Zurückführen automatisiert durch das Regelwerk erfolgen.

Der macmon-eigene AntiVirus Konnektor ist Teil von macmon Compliance und erlaubt die Anbindung diverser Antivirus-Systeme wie F-Secure, G Data, Kaspersky, McAfee, Sophos, Symantec oder TrendMicro, um auf kritische Events reagieren zu können, ohne notwendige Konfigurationen selbst vornehmen zu müssen. Betroffene Clients werden schnellstmöglich aus dem Netzwerk ausgesperrt – wenn gewünscht, durch das Herunterfahren des Switchports sogar physikalisch – ‚man wird umgehend über die Maßnahme informiert und erfährt, um welches Endgerät es sich handelt und wo es sich befindet. Der Administrator wird in die Lage versetzt, das betroffene System in aller Ruhe säubern und wieder in Betrieb nehmen zu können. Wenn das Antivirus-System auf einem Endgerät meldet, dass eine Malware nicht gesäubert und nicht gelöscht werden konnte, möchte man das betreffende System möglichst schnell finden und isolieren, um händisch eingreifen zu können. Der Konnektor erkennt diese Situation und verändert den Status eines betroffenen Endgeräts auf „non-compliant“, um es selbsttätig in einen Quarantäne-VLAN oder auch Remediation-VLAN zu isolieren und es in diesem geschützten Umfeld hinsichtlich des Sicherheitsstatus zu aktualisieren bzw. von Schadsoftware zu befreien. Zudem kann ein definierter Personenkreis informiert werden.

Erfahren Sie mehr darüber, wie macmon Sie bei der Umsetzung der DSGVO unterstützen kann (pdf): https://www.macmon.eu/fileadmin/users_all/content/Produktinfos/DEU_Datenblaetter/macmon_NAC_Datenschutzgrundverordnung_12_12_2017.pdf

Über macmon secure

Die macmon secure GmbH bietet komfortable und intelligente Netzwerkzugangskontrolle made in Germany, um Netzwerke vor unberechtigten Zugriffen zu schützen. Die Lösung besitzt ein BSI-Zertifikat und erfüllt die Anforderungen von KRITIS-Umgebungen.
https://www.macmon.eu/