Redaktion: Helmut Reimer

Report

VPN Management System mit neuen Funktionen

Der am 29. März 2022 vorgestellte NCP Secure Enterprise Management Server („SEM") ist als zentrale Komponente der „Single Point of Administration" der NCP VPN Enterprise-Lösung. Mit ihm können Unternehmen ihr Remote Access-Netzwerk bequem von zentraler Stelle aus administrieren und müssen sich nicht mit einer Vielzahl an Insellösungen beschäftigen. In der neuen Version 6.10 profitieren „SEM"-Administratoren von einer REST API sowie einer zubuchbaren Lizenz Option für die Zwei-Faktor-Authentisierung. Außerdem ist der „SEM" 6.10 für den Einsatz mit der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassenen NCP VS GovNet-Lösung geeignet.

Der „SEM" unterstützt ab Version 6.10 die Schnittstelle REST API (Representational State Transfer – Application Programming Interface). Diese versetzt Administratoren in die Lage, Statusinformationen vom System abzufragen oder Befehlsskripte an den „SEM" zu übertragen. Besonders hervorzuheben ist eine im Lieferumfang enthaltene NCP „SEM" API für Python, welche Anwendern eine leistungsfähige Schnittstelle zum „SEM" bereitstellt.

Die Zwei-Faktor-Authentisierung nach TOTP- oder SMS-Verfahren kann im „SEM" 6.10 als kostenpflichtige Lizenz-Option hinzugebucht bzw. aktiviert werden. Danach kann mit dem NCP Secure Enterprise Management Server entweder ein Time-based One-time Password (TOTP) oder alternativ eine SMS als zweiter Faktor für die VPN-Einwahl zur Verfügung gestellt werden. Zur Erzeugung des Einmalpasswortes nach dem TOTP-Verfahren auf Anwenderseite ist ein Software-Token notwendig. Dieser kann mit der NCP Authenticator App generiert werden, welche im Apple Store sowie im Google Play Store für Smartphones und Tablets zum kostenlosen Download zur Verfügung steht. Für zusätzliche Sicherheit kann die NCP Authenticator App eine biometrische Authentifizierung (Fingerabdruck- oder Gesichtserkennung) vor der Freischaltung des Passcodes verlangen.

Der „SEM" 6.10 kann für die Administration des NCP VS GovNet Connectors verwendet werden. Dabei handelt es sich um einen vom Bundesamt für Sicherheit in der Informationstechnik für VS-NfD zugelassenen Software-Client für Windows 10. Anwender können dadurch von den Vorteilen der zentralen Administrierbarkeit profitieren. Für einen vollumfänglichen VS-NfD-Arbeitsplatz kann die NCP VS GovNet-Lösung bestehend aus zwei Softwarekomponenten verwendet werden:

- NCP VS GovNet Connector mit-BSI-Zulassung für „VS-NfD", „RESTREINT UE/EU RESTRICTED" und „NATO RESTRICTED"
- NCP Secure VPN GovNet Server mit BSI-Zulassung für VS-NfD.

Beide Komponenten sind im Einsatzverbund ideal für sichere Bearbeitung und Übertragung sensibler Daten im Rahmen der genannten Geheimhaltungsstufen geeignet.

Darüber hinaus löst das NCP Secure Enterprise Management 6.10 das NCP Exclusive Remote Access Management ab. Dadurch werden die auf Juniper SRX Gateways abgestimmten NCP Exclusive Remote Access Clients nun auch mit dem „SEM" zentral verwaltet.

Die NCP Remote Access Lösung bietet auch große Flexibilität hinsichtlich der Lizenzierung. So kann die Lösung neben der herkömmlichen Kauflizenz auch mit einer flexiblen Pay-per-Use-Lizenz betrieben werden. Gerade in Pandemiezeiten wurde diese Variante von den Kunden als sehr flexibel ausgewählt.

Die Rolle nationaler Cybersicherheitsagenturen für die digitale Souveränität Europas

In letzter Zeit wurde viel über die Cybersicherheit „made in Europe" berichtet, wobei öfters die Leistung der nationalen Sicherheitsbehörden für Informationssysteme hervorgehoben worden ist. Als Beispiel wird insbesondere die Arbeit der französischen ANSSI und des deutschen BSI als nachahmenswert in Ländern ohne eine solche Behörde angeführt. Stormshield, renommierte europäische Referenz im Bereich Cybersecurity, hebt am 25. März 2022 die Vorteile der ANSSI-Qualifikation für seine Lösungen hervor und beleuchtet mit Marco Genovese, Presales-Specialist für die Industrial-Business-Line, einige potenziell unklare Punkte für diejenigen, die nicht genau wissen, was die ANSSI-Qualifikation tatsächlich beinhaltet.

Zertifizierung und Qualifizierung: Der Code muss übergeben werden

„Zunächst einmal gibt es einen großen Unterschied zwischen der Zertifizierung (die ANSSI „CSPN" oder „Sicherheitszertifizierung der ersten Stufe" nennt) und der Qualifizierung", beginnt Genovese. Im Fall der CSPN-Zertifizierung wird das Produkt als Blackbox betrachtet. Es wird nicht auf den Code oder auf Produktionsverfahren eingegangen, sondern überprüft, ob die Angaben im Benutzerhandbuch wahrheitsgetreu sind. Dazu zählen etwa offene Ports, die eigentlich geschlossen sein sollten, und ähnliche Ungereimtheiten.

Bei der Qualifizierung eines Cybersicherheitsproduktes hingegen geht es um die Funktionen, den Code und den gesamten Produktionsablauf. Die ANSSI analysiert nicht nur das Produkt, sondern schreibt dem Anbieter auch die Entwicklung bestimmter Funktionen vor, die sie für die Gewährleistung der Sicherheit sensibler Netze für unverzichtbar hält. Beispielhaft sei hier die Implementierung bestimmter Verschlüsselungsalgorithmen genannt. Außerdem müssen veraltete Funktionen oder Algorithmen, die versehentlich oder missbräuchlich eingesetzt werden könnten, entfernt werden oder wenigstens sperrbar sein.

Doch nicht nur das: „Der Code der Lösung muss an die Behörde geliefert werden, weshalb viele Anbieter vor der Qualifizierung zurückschrecken", erklärt Genovese. Sind Teile des Codes angreifbar, sucht ANSSI eine Lösung mit dem Anbieter. Diese Interaktion findet auch dann statt, wenn ANSSI der Ansicht ist, dass Teile des Codes besser geschrieben werden könnten. Die Agentur analysiert darüber hinaus den gesamten Fertigungsprozess und empfiehlt bewährte Verfahren, woran sich der Anbieter bei der Überprüfung der Korrektheit und Qualität des entwickelten Codes orientieren soll.

Zu guter Letzt kann die ANSSI die Qualifizierung jederzeit widerrufen, falls die Lösungen nach ihrer Qualifizierung Schwachstellen aufweisen, die nicht kurzfristig durch Workarounds oder Fixes behoben werden können.

Ein Prozess mit erheblichen Implikationen für die Anbieter

Dieses Verfahren ist zwar nur in groben Zügen umrissen, hat aber bedeutende Auswirkungen auf einen Anbieter.

Die Analyse des Codes einer Lösung nimmt mindestens ein Jahr in Anspruch. „Nehmen wir unsere Geräte als Beispiel: Allein der Konfigurationsassistent für die Version 3 unserer Firmware besteht aus 10.000 Codezeilen", sagt Genovese. „Während der Analyse kann die ANSSI verlangen, dass ein Teil dieses Codes aus Sicherheitsgründen geändert und anschließend einer erneuten Prüfung unterzogen wird, was die für die Analyse erforderliche Zeit weiter verlängert."

Ein weiteres Merkmal der Qualifizierung ist, dass sie an die von ANSSI geprüfte Hard- und Firmware gebunden ist. Somit ist das Hardware-Modell A mit der Firmware-Version B qualifiziert. Wird ein Upgrade auf Version C durchgeführt, ist das Produkt nicht mehr qualifiziert.

All dies bedeutet, dass ein Hersteller seinen gesamten Fertigungsprozess, seinen Produktlebenszyklus und sogar seine Logistik und Bevorratung anpassen muss. Ziel ist es, bestimmte Plattformen über längere Zeiträume zu unterstützen als die normalen Lebenszyklen eines nicht qualifizierten Sicherheitsproduktes.

Darüber hinaus ist der Gesamtablauf äußerst aufwendig und bedingt auch Änderungen der Roadmap. Genovese erklärt die Konsequenzen ganz klar: „Das Verfahren ist weder mit den typischen Niedrigpreis-Ausschreibungsverfahren noch mit abstrusen Buzzword-orientierten magischen Quadranten, Spiralen oder Dreiecken kompatibel. Als Anbieter ist man verpflichtet, Ressourcen in Sicherheitsfunktionen zu investieren, die auf den ersten Blick keine Highlights zu sein scheinen, bis man plötzlich Military-Grade-Lösungen wie die unseren benötigt oder eine schwerwiegende Schwachstelle in Wettbewerbsprodukten aufgedeckt wird. In solchen Fällen ist man dafür dankbar, mehr Ressourcen in die Abhärtung der Lösungen und weniger in Marketing-wirksame Cyberlappalien investiert zu haben."

Ein zu vermittelnder Mehrwert

Trotz dieser Aspekte stellt ein gut von einer nationalen Sicherheitsbehörde durchgeführtes Qualifizierungsverfahren einen unbestrittenen Mehrwert dar, insbesondere wenn das zu diskutierende Thema echte Cybersicherheit ist. Nationale Behörden oder Agenturen wie die ANSSI oder das BSI, die Richtlinien vorgeben, sind daher zu begrüßen. Der Mehrwert einer solchen Qualifizierung muss jedoch auch vom Kunden wahrgenommen werden. Andernfalls verlieren die Unternehmen, die sich auf einen solchen Prozess einlassen, an Wettbewerbsfähigkeit. Selbst in Frankreich gibt es trotz der enormen Aufklärungsbemühungen der ANSSI immer noch zahlreiche Unternehmen, die mehr auf Preis und „Pailletten" als auf den Inhalt achten. Hingegen sollte man in der Lage sein, die Richtlinien der Zertifizierungsstelle zu befolgen und den Wert der damit verbundenen Arbeit zu erkennen.

Die von Genovese erwähnten Aktivitäten sind nur ein kleiner Teil der Aufgaben der ANSSI. So veröffentlicht ANSSI zum Beispiel auch Merkblätter über den richtigen Einsatz qualifizierter Technologien. „Denn man kann die sicherste Lösung der Welt erwerben, aber wenn man sie oberflächlich einrichtet, lohnt sich die Anschaffung kaum", so Genovese abschließend.

Cybersicherheit –jeder Dritte fürchtet Cyberattacke auf seinen Arbeitgeber

Unternehmen sind und bleiben ein attraktives Ziel für kriminelle Hacker. Daher überrascht es nicht, dass jeder dritte Angestellte für seinen Arbeitgeber das Risiko hoch einschätzt, einer Cyberattacke zum Opfer zu fallen. Das zeigt die aktuelle, am 24. März 2022 veröffentlichte, Umfrage „Cybersicherheit in Zahlen" von G DATA CyberDefense. Was aber überrascht: Die Bewertungen zwischen kleinen und großen Unternehmen gehen deutlich auseinander.

Wie real die Gefahr von Cyberattacken auf Unternehmen ist, zeigt die aktuelle Umfrage von G DATA CyberDefense in Zusammenarbeit mit Statista. Jeder dritte Befragte schätzt das Risiko, dass sein Arbeitgeber zum Ziel einer Cyberattacke wird, als hoch ein. Demgegenüber schätzen nur 28 Prozent die Gefahr als gering ein. Dabei vergeht kaum ein Tag, an dem nicht über einen aktuellen erfolgreichen Cyberangriff auf ein Unternehmen berichtet wird. Allerdings unterscheidet sich die Risikobewertung erheblich von der Größe des Unternehmens. So schätzen nur 20 Prozent der Befragten aus einem Unternehmen mit weniger als 50 Mitarbeitenden die Gefahr einer Cyberattacke auf ihren Arbeitgeber als hoch ein. Bei Unternehmen mit mehr als 1.000 Unternehmen sind es mehr als 44 Prozent, die das Risiko eines Cyberangriffs auf ihren Arbeitgeber als hoch bewerten.

„Kleine Unternehmen unterliegen immer noch dem Irrglauben, dass sie kein attraktives Ziel für kriminelle Hacker sind", sagt Tim Berghoff, Security Evangelist bei G DATA CyberDefense. „Dabei bestimmen die Angreifer, ob ein Angriff lohnt und Profit bringt. Daher ist IT-Sicherheit keine Frage der Unternehmensgröße. Auch kleine und mittelständische Unternehmen müssen in IT-Sicherheit investieren und sich vor Angriffen schützen. Und das besser heute als morgen."

Je größer das Wissen, desto größer die Angst

Die Studie zeigt auch, dass die Risikoeinschätzung stark vom IT-Sicherheitswissen der befragten Personen abhängt und sich deutlich unterscheidet. So liegt der Anteil der Befragten mit sehr großer IT-Sicherheitskompetenz bei 57 Prozent, die ein hohes Angriffsrisiko für ihren Arbeitgeber sehen. Demgegenüber schätzen nur 15,2 Prozent der Befragten mit wenig IT-Sicherheitswissen die Gefahr als hoch ein, dass ihr Arbeitgeber ins Visier von Cyberkriminellen gerät. Es ist davon auszugehen, dass Menschen mit umfassenden IT-Sicherheitskompetenzen die Gefahren besser einschätzen können, weil sie die Zusammenhänge der IT-Sicherheit im Unternehmen besser nachvollziehen können. Und somit auch die potenziellen Schwachstellen sehen. Daher sollten Unternehmen die IT-Sicherheitskompetenzen ihrer Belegschaft stärken. Denn dann können die Mitarbeitenden diese potenzielle Cybergefahren frühzeitig erkennen und einen erfolgreichen Angriff verhindern.

Die Studie „Cybersicherheit in Zahlen" zeichnet sich durch eine hohe Informationsdichte und besondere methodische Tiefe aus: Mehr als 5.000 Arbeitnehmer*innen in Deutschland wurden im Rahmen einer repräsentativen Online-Studie zur Cybersicherheit im beruflichen und privaten Kontext befragt. Die Experten von Statista haben die Befragung durchgeführt und können dank einer

Stichprobengröße, die weit über dem branchenüblichen Standard liegt, belastbare und valide Marktforschungsergebnisse im Heft „Cybersicherheit in Zahlen“ präsentieren.

Studie „Cybersicherheit in Zahlen“ zum Download: *https://www.gdata.de/weka-studie-cyber-security*

Das Magazin „Cybersicherheit in Zahlen gibt es zum Download unter: *www.gdata.de/cybersicherheit-in-zahlen*

Bundesverband IT-Sicherheit e.V. (TeleTrusT): Gemeinsame Kraftanstrengung zur Verbesserung der IT-Sicherheit

Angesichts der veränderten geopolitischen Situation infolge des Ukraine-Konfliktes fordert der Bundesverband IT-Sicherheit (TeleTrusT) am 24. März 2022 von Politik, Regulierern und Betreibern weitreichende IT-Sicherheitsmaßnahmen und Investitionen zur Verbesserung der nationalen Sicherheit und der Versorgungssicherheit.

Cyberangriffe auf Unternehmen, staatliche Einrichtungen und kritische Infrastrukturen der Ukraine haben gezeigt, dass kritische Infrastrukturen und industrielle Netzwerke zunehmend in den Fokus politisch motivierter Cyberattacken geraten.

Energiewende und Digitalisierung der Produktion erfordern starke IT-Sicherheit

Die Beschleunigung der Energiewende und die zunehmende Vernetzung der Industrieproduktion einschließlich Logistik und Supply Chain erfordern zwingend ein hohes Maß an Digitalisierung und erhöhen damit auch das Risiko, zu einem potentiellen Angriffsziel von politisch motivierten Hackern zu werden.

Steffen Heyde, secunet, Leiter der TeleTrusT-AG „Smart Grids/Industrial Security“: „Die neue geopolitische Lage, ausgelöst durch den Ukraine-Konflikt, ist Zäsur und Zeitenwende auch für die IT-Sicherheit in Deutschland. IT-Sicherheit ist ein entscheidender Pfeiler der nationalen Sicherheit und letztendlich Garant der Aufrechterhaltung von Versorgungssicherheit und des Funktionierens unserer Volkswirtschaft auch in Krisenzeiten.“

Konzertierte Aktion zur Anhebung des IT-Sicherheitsniveaus erforderlich

TeleTrusT fordert daher eine engagierte nationale Kraftanstrengung von Politik, Regulierern und Betreibern zur Verbesserung der Cybersicherheit und der nationalen Sicherheit:

- Beschleunigung der Energiewende und schnelle Digitalisierung mit einem sehr hohen Security Level;
- Nachschärfung des IT-Sicherheitsgesetzes auf ein höheres Sicherheits- und Vertrauensniveau;
- Strengere Prüfung der Umsetzung des höheren Sicherheitslevels durch Auditoren bei Versorgungsunternehmen (KRITIS);
- Pragmatische, unbürokratische Unterstützung und Förderung der KMUs bei der Bewältigung der IT-Sicherheitslage;
- Wirksame Absicherung der Industrieproduktion und digitaler Industrie-Netzwerke, einschließlich Logistik und Supply Chain;
- Beachtung der Vertrauenswürdigkeit von IT-Sicherheitslösungen bei Kaufentscheidungen;
- Verbesserung des Qualifizierungsniveaus des Personals in Bezug auf IT-/OT-Sicherheit.

Sieben Schutzmaßnahmen gegen Cyberattacken auf Unternehmen

Was bereitet Unternehmen weltweit im Jahr 2022 am meisten Sorge? Noch vor Geschäftsunterbrechungen oder Naturkatastrophen liegen mittlerweile Cybergefahren, wie das jüngste Allianz Risk Barometer[1] zeigt. Aus gutem Grund: Das Bundeslagebild Cybercrime 2020 des Schweizerischen Bundeskriminalamts weist für 2020 erneut eine Steigerung der Cybercrime-Delikte gegenüber dem Vorjahr auf, und dieser Trend hält an. Nevis, ein Schweizer Spezialist für Identity und Access Management-Lösungen, gibt am 24. März 2022 Tipps, was Unternehmen im Rahmen einer guten Cybersicherheitsstrategie beachten sollten.

Die Gründe dafür, warum die Zahl der Cyberattacken weltweit immer weiter steigt, sind vielfältig. Zum einen sind sie eine Folge der voranschreitenden Digitalisierung, die coronabedingt noch einmal Fahrt aufgenommen hat. Zum anderen werden die Täter immer professioneller und viele Schadprogramme sind immer schwieriger zu entdecken. Besonders Attacken mit Ransomware stellen weiterhin eine große Gefahr für Unternehmen und Behörden dar. Diese Angriffsmethode sehen 57 Prozent der Befragten im Allianz Risk Barometer als größte Cyberbedrohung für das kommende Jahr an. Besorgniserregend ist in diesem Zusammenhang, dass die sogenannte Double Extortion immer beliebter wird. Dabei werden die Daten nicht nur verschlüsselt und erst gegen Zahlung eines Lösegeldes die Entschlüsselung gewährt. Sie werden gleichzeitig gestohlen und die Rückgabe ebenfalls von einer Geldzahlung abhängig gemacht. Die Opfer haben allerdings keine Garantie, dass ihre Informationen nicht trotzdem weiterverkauft werden. Bei Cyberkriminellen ist Ransomware vor allem beliebt, weil ihr Einsatz kostengünstig ist und keine großen technischen Kenntnisse erfordert.

Sieben Schutzmaßnahmen

Um sich vor Ransomware und anderen Angriffsmethoden zu schützen, sollten Unternehmen im Sinne ihrer Cybersicherheit folgende Punkte beachten:

1. State-of-the-Art-Lösungen unter anderem für die Endpunktesicherheit, den Schutz vor Trojanern und Viren oder den besonders gefährdeten Login-Bereich sind das A und O in Sachen Cyber-Sicherheit.
2. Alle Daten sollten regelmäßig auf Offline-Medien gesichert werden. Nur so sind sie vor dem Zugriff von Online-Kriminellen sicher geschützt.
3. Betriebssysteme und Software müssen regelmäßig aktualisiert werden. Produkte, die keine Sicherheitsunterstützung mehr vom Hersteller erhalten, müssen durch neuere ersetzt werden.
4. Bei jedem Klick auf per E-Mail geschickte Anhänge und Links ist Vorsicht gefragt, insbesondere wenn Anhänge dazu auffordern, bestimmte Prozesse zuzulassen, zum Beispiel das Ausführen von Makros. Links sollten lieber direkt in die Browserzeile eingegeben werden.
5. Manche Browser-Plugins beinhalten Sicherheitslücken, die Cyberkriminelle ausnutzen. Daher ist es empfehlenswert, diese Plugins zu deaktivieren.
6. Jedes Unternehmen sollte über ein Notfallkonzept für den Fall einer erfolgreichen Cyberattacke verfügen. Darin sind Verantwortlichkeiten, Kommunikationswege und Abläufe definiert. Dies hilft Schäden einzudämmen.

1 www.allianz.com/en/press/news/studies/220118_Allianz-Risk-Barometer-2022.html

7. Unternehmen tun gut daran – insbesondere in Zeiten von Remote Work – ihre Mitarbeiter für die wachsenden Gefahren von Cyberangriffen zu sensibilisieren. Dafür eignen sich Schulungen und Sicherheitstrainings.

Generell ist festzuhalten: Wenn es um ihre Cybersicherheit geht, ist es für Unternehmen nicht mit der einmaligen Anschaffung einer wirksamen Sicherheitslösung getan. Die Zahl der Attacken wird weiter zunehmen und die Methoden der Cyberangreifer immer raffinierter werden. Der Schutz von Unternehmens-IT und der Daten ist daher ein Thema, bei dem es gilt, kontinuierlich auf der Hut zu sein, die Entwicklungen zu beobachten und im Zweifel weitere Gegenmaßnahmen zu ergreifen.

Cloud-Automatisierung: Schlüssel für zukunftsfähige Cybersecurity

Die Mehrheit der IT-Entscheider sieht in Cloud Automation einen wichtigen Schlüssel zu einer zukunftsfähigen Cybersicherheit, vor allem in Kombination mit autonomen Privilegien und Zugriffen. Dies ist das Ergebnis einer aktuellen Umfrage von Delinea, einem führenden Anbieter von Privileged-Access-Management (PAM)-Lösungen. So suchen 86 Prozent der Befragten derzeit nach Möglichkeiten, Zugriffskontrollen zu automatisieren, insbesondere bei privilegierten Zugängen. Gleichzeitig erhöhen die Unternehmen auch ihre Ressourcen, um der wachsenden Bedrohungslandschaft gerecht zu werden. 68 Prozent der Befragten gaben demnach an, sowohl ihr IT-Budget als auch IT-Personal 2022 aufzustocken.

Der am 23. März 2022 veröffentlichte Bericht „Cloud Automation is the Key to Future-Proofing Cybersecurity“[2] basiert auf den Antworten von mehr als 300 IT-Entscheidungsträgern, die im Februar 2022 im Auftrag von Delinea vom globalen Forschungsunternehmen Censuswide befragt wurden. Er skizziert wichtige Erkenntnisse für die Entwicklung einer Sicherheitsstrategie, die zukünftiges Wachstum unterstützt, und gibt Tipps, wie man sich in der komplexen und ständig verändernden Cybersicherheitslandschaft zurechtfindet. Future-proofing, dt. Zukunftsfähigkeit, meint in diesem Zusammenhang Produkte, Dienste oder technologische Systeme, die so konzipiert sind, dass sie im Laufe der Zeit ohne wesentliche Aktualisierungen weiter funktionieren und daher auch im Kampf gegen künftige Cyber-Bedrohungen eingesetzt werden können. Auf diese Weise umgehen Unternehmen die Notwendigkeit, Systeme und Infrastrukturen immer wieder anpassen oder auswechseln zu müssen.

Unsicherheits-Faktor Cloud

Mit der zunehmenden Migration von lokalen Systemen zu hybriden oder Multi-Cloud-Umgebungen, steigt auch die Komplexität bei der Verwaltung der verschiedenen IT-Umgebungen. IT-Teams stehen vor der Herausforderung, konsistente Sicherheitsrichtlinien zu implementieren und zu managen. Dies spiegelt sich auch im Report wider: So gaben 59 Prozent der Befragten an, dass ihre Hauptmotivation, Zugriffssicherheit in diesem Jahr zukunftsfähig zu gestalten, in den immer komplexeren Multi-Cloud-IT-Umgebungen liegt.

Cybersicherheit: Vorstellung versus Realität

Eine weitere Erkenntnis des Reports ist, dass viele Unternehmen die Wirksamkeit ihrer eigenen Sicherheitsmaßnahmen nach wie vor überschätzen. Trotz Herausforderungen wie zunehmende Ransomware-Angriffe oder eine hybrid-arbeitende Belegschaft, sind viele IT-Verantwortliche überzeugt, auf Cyberangriffe gut vorbereitet zu sein: 83 Prozent von ihnen sind demnach zuversichtlich, dass ihre derzeitigen Zugriffskontrollen den Anforderungen gerecht werden, und 71 Prozent glauben, dass sie sich schnell von einem Cyberangriff erholen können.

Auch in ihr PAM scheinen die Befragten Vertrauen zu haben: 69 Prozent halten ihr derzeitiges Sicherheitskonzept für privilegierte Zugriffe für sehr ausgereift bzw. ausgereift und fast 90 Prozent denken, dass sie in der Lage sind, unautorisierte privilegierte Aktivitäten zu überwachen und zu melden.

Die Realität zeigt dabei eine dramatischere Lage: So geben zwei von drei Unternehmen zu, bereits Opfer von Cyberangriffen geworden zu sein. Außerdem dauert es im Durchschnitt 280 Tage, um eine Datenschutzverletzung zu identifizieren und einzudämmen, wie der Cost of a Data Breach Report von IBM offenbart.

„Der aktuelle Report weist ein Paradox auf, wenn man bedenkt, dass sich der Großteil der Befragten in Bezug auf ihre derzeitigen Cybersicherheitsmaßnahmen sicher fühlt, obwohl die Zahl der Sicherheitsverletzungen, die durch kompromittierte Anmeldedaten verursacht wird, beträchtlich ist. Dennoch sind sich die IT-Entscheider bewusst, dass die Zukunft ihrer Unternehmenssicherheit in der Cloud-Automatisierung liegt, was für die meisten einen dynamischen Umbruch in Bezug auf Herangehensweise, Investitionen und Ressourcen bedeutet“, so Joseph Carson, Advisory CISO und Chief Security Scientist bei Delinea. „Die Cyberbedrohungen von heute sind schneller, intelligenter und gefährlicher. Um Sicherheitsprobleme zu vermeiden und in der heutigen unvorhersehbaren Landschaft zu überleben, bleibt Unternehmen kaum ein anderer Weg, als sich stark auf die Automatisierung stützen und Best Practices wie Least Privilege und Zero Trust auf Schritt und Tritt umzusetzen.“

Empfehlung

Basierend auf den Ergebnissen des Reports rät Delinea Unternehmen, ihre Zukunftsfähigkeit auf Cloud-Automatisierung und autonomen privilegierten Zugriffen aufzubauen. Gleichzeitig sollten sie sich von manuellen und komplexen Workflows verabschieden, die Geschäftsprozesse verlangsamen.

Die vollständigen Report-Ergebnisse stehen zum Download bereit: *https://delinea.com/news/research-delinea-future-proofing-cybersecurity*

3G-Nachweis und Kontaktdaten – einfach zerreißen reicht nicht!

Mit der Änderung des Infektionsschutzgesetztes vom 20. März 2022 entfällt die Verpflichtung zum Nachweis der Impfung, der Genesung oder der Negativ-Testung (3G-Nachweis) am Arbeitsplatz. „Die aktuellen Lockerungen im Rahmen des Infektionsschutzgesetzes des Bundes nimmt die Landesbeauftrage für Datenschutz und Informationsfreiheit in Nordrhein-Westfalen am 23. März 2022 zum Anlass, um auf Fristen für die Löschung der gesammelten Daten hinzuweisen: Die von den Arbeitgeber*innen erhobenen Daten müssen spätestens sechs Monate nach Erhebung vernichtet oder gelöscht werden. Da die Rechtsgrundlage entfallen ist, gehen wir davon aus,

2 https://delinea.com/news/research-delinea-future-proofing-cybersecurity

dass die Speicherung regelmäßig nicht mehr erforderlich ist und die Daten schon jetzt gelöscht werden sollten", erklärt Bettina Gayk.

Angesichts steigender Corona-Zahlen gewann für Unternehmen die Erfassung von Gesundheitsdaten der Beschäftigten an Bedeutung, um den Betrieb trotz der Risiken durch SARS-CoV-2 aufrechtzuhalten. Dabei wurden die Arbeitgeber*innen verpflichtet zu überwachen, ob die Beschäftigten geimpft, genesen oder getestet sind. Dazu sollte eine tägliche Nachweiskontrolle durchgeführt und dokumentiert werden. Geregelt wurde das durch das Infektionsschutzgesetz des Bundes (§ 28b Abs. 3 Satz 1 IfSG a.F.). „In Einzelfällen haben Arbeitgeber*innen Impf- oder Testnachweise sogar kopiert oder gescannt. Das ist nicht zulässig gewesen, und selbstverständlich müssen diese Kopien und Scans umgehend fachgerecht entsorgt werden", macht Gayk deutlich.

Dass im Zuge der Pandemie gesammelte Daten wieder gelöscht oder vernichtet werden müssen, ist nicht neu. So ist bereits die Pflicht zur Kontaktdatenerhebung für bestimmte Wirtschaftsbereiche – zum Beispiel in der Gastronomie – entfallen, als am 20. August 2021 die „Verordnung zum Schutz vor Neuinfizierungen mit dem Coronavirus SARS-CoV-2" (Corona-Schutzverordnung) der NRW-Landesregierung geändert wurde. Allerdings kann sie seitdem noch weiterhin durch die Städte und Gemeinden als örtliche Ordnungsbehörden angeordnet werden.

Gayk: „Inzwischen geht es darum, die erhobenen Daten rechtskonform zu entsorgen. Das bedeutet: Die Gesundheitsdaten von Beschäftigten und – sofern noch vorhanden – Daten zur Kontaktnachverfolgung müssen gelöscht, also vollständig und unwiderruflich vernichtet werden. Bei Daten, die in Papierform erhoben wurden, sollte ein geeigneter Aktenvernichter verwendet werden." Ein Zerreißen von Hand sei nicht ausreichend. Wie Datenträger datenschutzkonform vernichtet werden können, regelt unter anderem die DIN 66399. Für das Löschen personenbezogener Daten durch Aktenvernichter sind Geräte der Sicherheitsstufe 4 oder höher gemäß dieser DIN geeignet.

Utimaco vervollständigt mit u.trust Data File sein Datenschutzportfolio

Utimaco, ein weltweit führender Anbieter von IT-Sicherheitslösungen, stellte am 15. März 2022 ‚u.trust Data File' für die Datenverschlüsselung vor. Mit der Erweiterung seines Portfolios um das neue Produkt bietet das Unternehmen seinen Kunden nun ein komplettes Lösungspaket für die IT-Sicherheit in den Bereichen Datenverschlüsselung, Hardware-Sicherheitsmodule, Schlüsselmanagement und Public Key Infrastruktur (PKI) an.

Der Schutz von Daten wird für Behörden und Unternehmen in allen Branchen immer wichtiger, da die rasant fortschreitende Digitalisierung und mobiles Arbeiten potenzielle neue Angriffsvektoren eröffnet. Durch die zunehmende Nutzung von cloudbasierten Diensten werden immer mehr Daten gemeinsam genutzt und extern gehostet. Unternehmen müssen daher ihre Daten unabhängig vom Speicherort schützen. Darüber hinaus machen Aufsichtsbehörden Unternehmen für die Nichteinhaltung von Standards im Bereich Datenverwaltung und Datenzugriff verantwortlich, die zu Verstößen gegen Datenschutzbestimmungen führen.

Mit ‚u.trust Data' File begegnet Utimaco diesen Herausforderungen. Die einfach zu integrierende softwarebasierte Lösung gewährleistet den konformen Umgang mit sensiblen Daten in Übereinstimmung mit Datenschutzbestimmungen wie DSGVO, CCPA, PDPA usw. Gleichzeitig ist sie benutzerfreundlich – ein entscheidender Faktor für die Akzeptanz von Sicherheitsmaßnahmen, da die Mitarbeiter keinen Unterschied in ihrer Arbeitsroutine bemerken werden.

Die Vorteile und Funktionen im Überblick:

- Rollenbasierte Verschlüsselung von sensiblen und unternehmenskritischen Daten
- Schutz von ruhenden Daten (Data at Rest) und Daten in der Übertragung (Data in Motion) mit persistenter Verschlüsselung
- Hohe Skalierbarkeit für alle Unternehmensgrößen in allen Branchen und für alle Dateitypen
- Flexible Implementierung verschiedener Schutzszenarien für unterschiedliche Datenschutzanforderungen
- Multi-Plattform-Ansatz: Windows (10 & Server inkl. Terminal), macOS, iOS, Android, Linux (geplant)
- Geeignet für Cloud und Multi-Cloud: unterstützt verschlüsselte Speicherung auf den gängigsten Cloud-Speicheranbietern wie Microsoft OneDrive, Google Drive, Amazon Cloud Drive oder Dropbox
- Vollständige Einrichtung einer verschlüsselten Umgebung in großen Unternehmen durch Definition von fünf bis sieben generischen Regeln
- Integration mit der Schlüsselverwaltung und den Hardware-Sicherheitslösungen von Utimaco für höchste Sicherheits- und Zertifizierungsstandards

„Unternehmen weltweit stehen immer wieder vor der Herausforderung, ihre unternehmenskritischen und sensiblen Daten zu schützen. Utimaco ‚u.trust Data File' bietet eine zuverlässige Datenverschlüsselung, ohne dass Mitarbeiter und Angestellte ihre Arbeitsabläufe anpassen müssen", kommentiert Mario Galatovic, Vice President Products & Alliances.

„Die Lösung ist einfach zu bedienen, bietet eine flexible Zugriffsverwaltung und eignet sich daher für alle möglichen Anwendungsfälle, bei denen es um Datenschutz geht. Mit dieser Produkteinführung bieten wir nun ein ganzheitliches Datenschutzportfolio an, das nahtlos ineinandergreift und unsere Position als zuverlässiger Partner und Anbieter für unsere Kunden weltweit stärkt", so Galatovic.

Neue OpenSSL Sicherheitslücke: IoT Inspector erkennt betroffene Software automatisch

Eine neue bedrohliche Sicherheitslücke gefährdet weltweit alle Systeme, die OpenSSL, eine der meistverwendeten Softwares für Verschlüsselung aller Art, zur Transportverschlüsselung auf TLS-Basis einsetzen. Bei der Verarbeitung von bestimmten TLS-Zertifikaten können gezielte Attacken Clients und Server zum vollständigen Stillstand bringen (DoS -Denial of Service). „Server, Clients und sonstige Geräte müssen sofort geprüft und nötigenfalls gepatcht werden. Da diese Software sehr verbreitet ist, ist die Mehrheit aller IT-Systeme – vom Server über Clients bis hin zum Internet der Dinge – betroffen. Wenn Hacker diese Lücke gezielt attackieren, kann es für Unternehmen und Institutionen sehr kritisch werden", warnt am 17. März 2022 Jan Wendenburg, CEO von IoT Inspector. Das Security-Unternehmen[3] betreibt die führende europäische Plattform

3 https://www.iot-inspector.com/

zur automatisierten Überprüfung von IoT-Firmware. Die jüngst bekannt gewordene Schwachstelle kann so auch in IoT- und IIoT-Geräten und -Infrastruktur, bzw. in deren Software gezielt aufgedeckt und so behoben werden.

Bedrohungsgrad: Hoch

In jüngster Vergangenheit deckte das Team von IoT Inspector zahlreiche Schwachstellen bei bekannten Hardwareherstellern auf. „Wir haben erlebt, dass nach der Veröffentlichung eines technischen Advisories Hacker gezielt begonnen haben, die adressierte Sicherheitslücke zu attackieren. Daher sollten Administratoren sofort prüfen, ob das Problem in ihren Netzwerken vorliegt", sagt Jan Wendenburg von IoT Inspector. Die Sicherheitslücke (CVE-2022-0778) ist mit dem Bedrohungsgrad „hoch" eingestuft. Entdeckt wurde sie von Tavis Ormandy, einem britischen White-Hat-Hacker, der aktuell bei Google als Teil des Project-Zero-Teams arbeitet. Betroffen von der Schwachstelle sind die OpenSSL-Versionen 1.0.2, 1.1.1 und 3.0. Administratoren, die OpenSSL einsetzen, sollten zeitnah eine der abgesicherten Ausgaben 1.1.1n oder 3.0.2 installieren.

Unberechenbare Situation

Schnelle Reaktionen sind vor allem vor dem Hintergrund internationaler Cyberattacken aufgrund des Ukrainekrieges angebracht, rät das Spezialistenteam von IoT Inspector: „Kritische Infrastrukturen, aber auch Unternehmen, sind aktuell gefährdeter denn je. Der aufgedeckte Einsatz europäischer Technologie in russischem Kriegsgerät zeigt, wie schnell Unternehmen heute im Kreuzfeuer stehen und eventuell in einen Feldzug von Anonymous-Hackern gezogen werden könnten. Die Situation ist unberechenbar", erklärt Wendenburg. Erst vor wenigen Tagen warnte das Bundesamt für Sicherheit in der Informationstechnik (BSI) bereits zum dritten Mal vor kriegsbedingten Attacken auf IT-Infrastrukturen. Dabei kann jede Komponente eines Netzwerkes als Einfallstor genutzt werden, sofern die Sicherheitslücken nicht durch gezielte Analysen identifiziert und anschließend behoben werden. IoT Inspector bietet nach den Warnungen des BSI weiterhin einen kostenlosen Sicherheitscheck für IoT/IIoT Endpoints aller Art in KRITIS-Infrastrukturen an, um die europäische Sicherheitsarchitektur bestmöglich zu schützen. Ein Firmware-Check dauert nur wenige Minuten und analysiert die relevanten Risiken.

BSI erteilt Firewall genugate 10.0 VS-NfD-Zulassung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die High Resistance Firewall genugate 10.0 Z am 16. März 2022 für die Geheimhaltungsgrade „Verschlusssachen – nur für den Dienstgebrauch" (VS-NfD), RESTREINT UE/EU RESTRICTED sowie NATO RESTRICTED zugelassen1. Diese aktuelle Version der IT-Sicherheitslösung unterstützt ab sofort eine REST-API sowie die zentrale Log-Auswertung über Elastic Stack. Staatliche Einrichtungen sowie Unternehmen mit sehr hohem Schutzbedarf können damit Administrationsaufgaben umfassend automatisieren, IT-Infrastrukturen weiter konsolidieren und gleichzeitig sensible Infrastrukturen zuverlässig gegen Cyber-Risiken absichern.

Automatisierte Verwaltung komplexer Firewall-Systeme

Technologie-Trends wie Cloud-Dienste, Remote-Anbindung oder die IT-Konsolidierung erhöhen auch im öffentlichen Sektor die Komplexität von IT-Systemlandschaften. Dies erschwert es IT-Administratoren zunehmend, Firewalls effizient zu verwalten und zu kontrollieren. Damit steigt auch das Risiko für Fehlkonfigurationen und Sicherheitslücken.

Um aufwändige Administrationsaufgaben über eine große Zahl von Appliances zuverlässig zu handhaben, unterstützt die neue Version 10.0 Z der genugate eine REST-API, die eine maschinenlesbare Definition nach dem OpenAPI-Standard bietet. Behörden und Unternehmen können die Firewall so in großem Maßstab einsetzen und Prozesse einfach und transparent automatisieren. Hierzu zählen das Anlegen von Host-Einträgen, der Abgleich von Regelwerken über mehrere Installationen, die Erstellung von Regeln zur Einbindung in eine Cloud-Infrastruktur oder die Regelwerksdokumentation für Audit-Zwecke.

Verbesserte Auswertung und Analyse von Log-Meldungen

Die genugate 10.0 Z unterstützt außerdem ein zentrales Logging über Elastic Stack. Die Anbindung an die auch als ELK-Stack bekannte Open-Source-Lösung erlaubt eine komfortable Auswertung, Analyse und Behandlung von Log-Meldungen mehrerer Firewalls über eine einzige Benutzerschnittstelle (GUI) sowie das Echtzeit-Monitoring sicherheitskritischer Funktionen. So lassen sich selbst bei hochkomplexen Systemen mit vielen Devices Warnmeldungen schnell lokalisieren, bewerten und Maßnahmen ableiten.

Web Application Security und sichere Software-Updates

Die genugate 10.0 Z ist ferner weltweit die einzige Web Application Firewall (WAF), die durch das BSI eine Zertifizierung nach Common Criteria (CC) EAL4+ mit AVA_VAN.5 (Advanced Methodical Vulnerability Analysis) erhalten hat. Die Bezeichnung AVA_VAN.5 steht für ein hohes Maß an Selbstschutz, durch den die Firewall nachweislich selbst Angreifern mit hohem Angriffspotential standhält. Besonders gefährdete Organisationen wie Sicherheitsbehörden, Militär oder Betreiber kritischer Infrastrukturen können somit ihre Server zuverlässig vor Angriffen schützen.

Als einzige Firewall am Markt verfügt genugate 10.0 Z außerdem über ein nach CC EAL4+ zertifiziertes Patch-Management. Dieses sorgt zusätzlich für einen besonders effektiven Schutz von Software-Maintenance-Prozessen wie Updates und Patches gegen Infiltrationsversuche.

1IT-Sicherheitsprodukte, die innerhalb von Verschlusssachen-IT (VS-IT) im Behördenumfeld Sicherheitsfunktionen übernehmen, sind vor ihrem Einsatz vom BSI zuzulassen. Die aktuelle BSI-Zulassung für genugate 10.0 Z ist gültig bis zum 2. Februar 2024.

Firewall- und Gateway-Lösungen von genua *https://www.genua.de/it-sicherheitsloesungen/firewalls-gateways*

Sicherheit und Nutzerfreundlichkeit

Wenn Unternehmen an Sicherheit denken, denken sie oftmals an Passwörter, Verschlüsselung und Hackerangriffe. Mit dem Übergang zu flexibler, hybrider oder vollständiger Fernarbeit gibt es viele neue Aspekte, die in der Sicherheitsgleichung auftauchen und vor allem auch den Anforderungen an Unternehmensstandards standhalten müssen. Business-Software hat dabei meist den Nachteil, dass die Nutzerfreundlichkeit vernachlässigt wird. Doch die Anwender sind mitunter nicht technikaffin, sodass Benutzeroberflächen nicht intuitiv bedienbar sind. Laut einer Untersuchung von Lünendonk sehen Unternehmen die Digital Experience zwar als

ein Schlüsselelement zur Kundengewinnung und -bindung, doch die Mehrheit der Unternehmen (65 Prozent) empfindet die Qualität ihrer digitalen Nutzererfahrung im Wettbewerbsvergleich jedoch nur „auf Augenhöhe". Als Vorreiter sieht sich nur jedes zehnte Unternehmen (9 Prozent).

Consumer-orientiert aber sicher vernetzen

Vor allem in den Bereichen Kommunikation und Support sind Menschen aus dem Privaten an Messenger, Videotelefonie und Social-Media-Apps gewöhnt und wünschen sich die gleiche intuitive Bedienbarkeit für Unternehmensanwendungen im Browser wie auch per App auf verschiedenen Geräten. Consumer-orientierte Usability spart am Ende Zeit und Geld gerade auch bei Unified-Communication-and-Collaboration-Tools (UCC) oder Remote-Support-Anwendungen, da die Nutzer einwandfrei remote mit Kollegen und Kunden kommunizieren können. Diese Plattformen müssen jedoch sicher sein, um sichere und private digitale Räume für Anrufe, Meetings, virtuelle Veranstaltungen, Supportanfragen und vieles mehr zu bieten.

UCC und Support sund für flexibles Arbeiten unverzichtbar, aber Systeme vor Ort sind teuer und ressourcenintensiv in der Wartung und Gewährleistung der Sicherheit. Cloud-basierte Systeme ermöglichen einen schlanken und nahtlosen Betrieb, da Infrastruktur und Know-how an den Anbieter ausgelagert werden. Die höhere Anwenderzufriedenheit ist dabei oft ein unterschätzter Aspekt, da Unzufriedenheit gerade im Cloud-Zeitalter zum schnellen Anbieterwechsel führen kann. Sicherheit und Datenschutz führen jedoch meist dazu, dass Cloud-Anwendungen an Komplexität zunehmen und zusätzliche Sicherheitshürden ausgerollt sind, um den Zugriff zu Apps und Dateien besser zu sichern. Hier gilt es von IT-Seite einen guten Kompromiss zu finden, um die Sicherheitsstandards im Unternehmen weiterhin hoch zu halten, den Mitarbeitern aber gleichzeitig einfach zu nutzende und schnell zugängliche Anwendungen zur Verfügung zu stellen.

GoTo zeigt, wie wichtig Datenschutz und Sicherheit zum Schutz persönlicher und vertraulicher Informationen gerade auch bei Kommunikations- und Supporttools ist und nennt drei unerlässliche Sicherheitsfunktionen, die eine UCC- oder Support-Lösung für den Business-Einsatz benötigt, um externe Datenzugriffe zu verhindern:

1. Konsolidierung in einer Anwendung

Für eine einheitliche Sicherheitsstruktur sorgen All-in-One-Lösungen für Unified Communications as a Service (UCaaS), Contact-Center-as-a-Service (CCaaS) und Remote-Support. Über sie führen Mitarbeiter Anrufe, Meetings und Nachrichten oder bearbeiten Supportanfragen in einer einzigen Plattform aus und wechseln innerhalb derselben Anwendung problemlos zwischen den Kanälen. Auch IT-Teams haben so nur ein einziges Verwaltungsportal und können die Einstellungen, die zuvor in verschiedenen Anwendungen erfolgten, gesammelt managen. Durch die Konsolidierung auf einen Anbieter profitieren Unternehmen von Konnektivität und Zuverlässigkeit und bieten oftmals eine Vielzahl von Integrationen mit bestehenden CRMs und Kollaborationstools wie Slack und Microsoft Teams.

2. Implementierung von Sicherheitskontrollen

Um die Kommunikations- und Supportinfrastruktur und die darin enthaltenen Daten zu schützen, gilt es branchenübliche Sicherheitskontrollen einzusetzen. Mithilfe von logischer Zugriffskontrolle oder einem Perimeterschutz-Tool vermindern Administratoren die Bedrohung durch unbefugten Anwendungszugriffen oder nicht autorisiertem Netzwerkverkehr. Cloud-Lösungen wie UCaaS oder CCaaS haben darüber hinaus den Vorteil, dass die Datenzentral gespeichert vorliegen und IT-Verantwortliche Backups zentral und automatisiert erstellen können. Neben dem Schutz vor Malware und einer Ende-zu-Ende-Verschlüsselung (E2EE) für die schriftliche und verbale Kommunikation gilt es vor allem auch Schwachstellenmanagement und monatliche Netzwerk-Scans zu betreiben, um die Nutzung der Remote-Work-Lösungen immer im Blick zu behalten. Mithilfe einer Protokollierung erhalten Administratoren in Verdachtsfällen einen Alarm und können einem missbräuchlichen Datenverkehr schnell entgegenwirken. Diese Funktionen erfolgen zum großen Teil im Hintergrund und beeinträchtigen die Nutzung der Kommunikationssoftware nur geringfügig, bieten aber ein hohes Maß an Sicherheit und Datenschutz.

3. Ein engagiertes Sicherheitsteam

Ein ausgereifter Business-Continuity-Plan stellt sicher, dass alle Produkt- und Betriebsteams auch dann voll funktionsfähig sind, wenn sie aus der Ferne arbeiten. Seit der COVID-19-Pandemie ist es ratsam die Netzwerkkapazität und die Fähigkeit, Datenverkehr zu verschieben, zu erhöhen. Nur so kann die IT-Abteilung einen Single Point of Failure vermeiden. Ein Monitoring aller Cloud-Dienste rund um die Uhr hilft dabei, die Datenschutz- und Informationssicherheitsstandards in Unternehmen zu erfüllen oder sogar zu übertreffen.

Leider kam es während der Pandemie und der Zunahme an Remote Work in den Unternehmen in vielen Branchen zu einem sprunghaften Anstieg bösartiger Cyberangriffe, darunter Malware, Phishing-Angriffe, gefälschte Websites, Spammer und Scammer. Laut BSI bewerten über 26 Prozent der befragten Unternehmen, die aktiv auf Cyber-Angriffe reagieren mussten, die Schäden als „existenzbedrohend" oder sehr „schwer" und es entstanden Schäden in Höhe von 52,5 Milliarden Euro durch Angriffe im Homeoffice. Solch hohen Schäden hilft eine implementierte risikobasierte Authentifizierung entgegenzuwirken. Denn Plattformen, die verdächtiges Verhalten in den Nutzerprofilen vor allem bei der Anmeldung per Fernzugriff von einem nicht-autorisierten Gerät erkennen, können Fremdzugriffe von Hackern vermeiden und geben der Unternehmens-IT ein zusätzliches Security-Layer. Autorisierte Nutzer innerhalb der Belegschaft hingegen profitieren von nutzerfreundlichen, einfachen Anmeldeprozessen via Single-Sign-on, um schnell Zugang zu Daten und virtuellen Meetings zu erhalten.

Weitere Informationen zu den Sicherheitsfeatures bei GoTo finden Sie unter *https://www.goto.com/de/why-goto/secure-unified-communications#*

EU: Gesetz über digitale Märkte (DMA): Einigung zwischen Rat und Europäischem Parlament

Der Rat und das Parlament haben am 25. März 2022 eine vorläufige politische Einigung über das Gesetz über digitale Märkte (DMA)[4] erzielt, das auf eine gerechtere und stärker wettbewerbsorientierte Gestaltung des digitalen Sektors abzielt. Durch eine letzte, abschließende technische Überarbeitung soll der Text in den kommenden Tagen fertiggestellt werden.

4 https://ec.europa.eu/info/sites/default/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf

Cédric O, Staatssekretär für Digitales

„In den letzten zehn Jahren musste die Europäische Union aufgrund bestimmter schädlicher Geschäftspraktiken sehr großer digitaler Akteure Geldbußen in Rekordhöhe verhängen. Das DMA ermöglicht ein direktes Verbot dieser Praktiken und wird für neue Akteure und europäische Unternehmen einen faireren und bestreitbareren Wirtschaftsraum schaffen. Diese Vorschriften sind entscheidend, um die digitalen Märkte anzukurbeln und zu öffnen, Verbrauchern eine größere Auswahl zu bieten, in der digitalen Wirtschaft eine bessere Wertverteilung zu ermöglichen und Innovation zu fördern. Die Europäische Union ist die erste, die diesbezüglich so entschlossen handelt, und ich hoffe, dass andere sich uns bald anschließen werden."

Im Gesetz über digitale Märkte sind klare Regeln für große Online-Plattformen vorgegeben. Damit soll sichergestellt werden, dass große Online-Plattformen, die bezüglich einer großen Zahl von Nutzern als „Gatekeeper" fungieren, ihre Position nicht missbrauchen, um anderen Unternehmen den Zugang zu diesen Nutzern zu versperren.

Welche Plattformen gelten als Gatekeeper?

Der Rat und das Europäische Parlament sind übereingekommen, dass eine Plattform als Gatekeeper gilt, wenn sie in den vergangenen drei Geschäftsjahren in der Europäischen Union einen Jahresumsatz von mindestens 7,5 Mrd. € erzielt hat oder ihr Börsenwert mindestens 75 Mrd. € beträgt und sie monatlich mehr als 45 Millionen in der Union niedergelassene oder aufhältige Endnutzer bzw. mehr als 10 000 in der Union niedergelassene gewerbliche Nutzer hatte.

Außerdem muss die Plattform in mindestens drei Mitgliedstaateneinen oder mehrere zentrale Plattformdienste betreiben. Zu diesen zentralen Plattformdiensten gehören Marktplätze und Stores für Software-Anwendungen, Suchmaschinen, soziale Netzwerke, Cloud-Dienste, Werbedienste, Sprachassistenzdienste und Browser.

Damit die Vorschriften der Verordnung verhältnismäßig sind, werden KMU nur in Ausnahmefällen als Gatekeeper eingestuft. Um sicherzustellen, dass diese Verpflichtungen zunehmend zur Anwendung kommen, wurde auch die Kategorie des „neu entstehenden Gatekeepers" vorgesehen, sodass die Kommission bestimmte Verpflichtungen auch Unternehmen auferlegen kann, deren Wettbewerbsposition zwar bereits nachgewiesen, aber noch nicht von Dauer ist.

Für die Gatekeeper gilt insbesondere, dass sie

- sicherstellen, dass die Nutzer berechtigt sind, Dienste der zentralen Plattform zu ähnlichen Bedingungen abzubestellen wie zu abonnieren,
- die Software für die wichtigsten Programme (z. B. Browsersoftware) bei der Installation des Betriebssystems nicht standardmäßig vorschreiben,
- die Interoperabilität der Basisfunktionen ihrer Instant-Messaging-Dienste sicherstellen,
- Anwendungsentwicklern gleichberechtigten Zugang zu den Hilfsfunktionen von Smartphones (z. B. NFC-Chips) einräumen,
- Verkäufern Zugang zu ihren Marketing- oder Werbeleistungsdaten auf der Plattform geben,
- die Europäische Kommission über von ihnen durchgeführte Übernahmen und Fusionen unterrichten.
- Sie werden jedoch nicht mehr in der Lage sein,
- die eigenen Produkte oder Dienste gegenüber jenen anderer Marktteilnehmer durch Ranking besser zu positionieren (Bevorzugung des eigenen Unternehmens),
- die im Zuge der Bereitstellung eines Dienstes erhobenen personenbezogenen Daten für die Zwecke einer anderen Bereitstellung wiederzuverwenden,
- unlautere Bedingungen für gewerbliche Nutzer einzuführen,
- bestimmte Software-Anwendungen vorzuinstallieren,
- Anwendungsentwickler zur Verwendung bestimmter Dienste (z. B. eines Zahlungssystems oder Identitätsanbieters) zu verpflichten, damit diese in Stores für Software-Anwendungen verlinkt werden.

Was passiert, wenn sich ein Gatekeeper nicht an die Vorschriften hält?

Wenn ein Gatekeeper gegen die gesetzlichen Vorschriften verstößt, droht ihm eine Geldbuße von bis zu 10 % seines weltweiten Gesamtumsatzes. Im Wiederholungsfall kann eine Geldbuße von bis zu 20 % seines weltweiten Gesamtumsatzes verhängt werden.

Wenn ein Gatekeeper systematisch, das heißt mindestens dreimal in acht Jahren, gegen die DMA-Vorschriften verstößt, kann die Europäische Kommission eine Marktuntersuchung einleiten und erforderlichenfalls verhaltensbezogene oder strukturelle Abhilfemaßnahmen verhängen.

Was, wenn die Plattform mit ihrer Einstufung als Gatekeeper nicht einverstanden ist?

Wenn eine Plattform gute Gründe gegen ihre Einstufung als Gatekeeper vorbringen kann, hat sie die Möglichkeit, die Einstufung im Rahmen eines besonderen Verfahrens, das der Kommission die Überprüfung der vorgebrachten Gründe ermöglicht, anzufechten.

Wer stellt sicher, dass die Gatekeeper die Vorschriften einhalten?

Im Interesse eines hohen Maßes an Harmonisierung im Binnenmarkt darf die Verordnung nur durch die Europäische Kommission durchgesetzt werden. Die Kommission kann beschließen, einen Dialog über die Regulierungsmaßnahmen aufzunehmen, um sich zu vergewissern, dass die Gatekeeper die von ihnen einzuhaltenden Vorschriften genau verstehen, und um gegebenenfalls deren Anwendung zu präzisieren.

Zur Unterstützung der Kommission und um ihr die Arbeit zu erleichtern, werden ein beratender Ausschuss und eine hochrangige Gruppe eingesetzt. Die Mitgliedstaaten können die nationalen Wettbewerbsbehörden ermächtigen, Ermittlungen wegen möglicher Zuwiderhandlungen einzuleiten und ihre Erkenntnisse der Europäischen Kommission zu übermitteln.

Um sicherzustellen, dass die Gatekeeper nicht gegen die DMA-Vorschriften verstoßen, sind in der Verordnung auch Bestimmungen gegen die Umgehung der Vorschriften vorgesehen.

Verbindung zum Gesetz über digitale Dienste

Die beiden Gesetzgeber waren sich darin einig, dass die mit der Erhebung von Daten durch Gatekeeper verbundenen wirtschaftlichen Bedenken Gegenstand der DMA sind, während umfassendere gesellschaftliche Belange im Gesetz über digitale Dienste (DSA) behandelt werden sollten. Eine Einigung über das DSA ist ebenfalls demnächst zu erwarten.

DSA und DMA sind die beiden Säulen der Regulierung des digitalen Bereichs. Sie entsprechen den europäischen Werten und dem europäischen Modell und bilden einen dem wirtschaftlichen und demokratischen Fußabdruck der Tech-Giganten angemessenen Rahmen.

Veranstaltungskalender

6 | 2022

Veranstaltungen Juni		
Zeit und Ort	**Thema der Veranstaltung**	**Veranstalter**
01. – 02. Juni 2022 Web-Seminar	Spezielle Prüfverfahrenskompetenz für § 8a BSIG – KRITIS-Kompetenzvermittlung	isits AG International School of IT Security Huestr. 30, 44787 Bochum Tel.:0234/927898-0; Fax: 0234-92/7898-20
07. – 08. Juni 2022 Online	Die Umsetzung der BAIT angemessen planen und konzipieren (DGI®) – Erwerben Sie die spezifischen Kenntnisse zur Umsetzung der „Bankaufsichtliche Anforderung an die IT (BAIT)“	Akademie der DGI Deutsche Gesellschaft für Informationssicherheit AG, Kurfürstendamm 57, 10707 Berlin Tel.: 030/31517389-10; Fax: 030/31517389-20
13. – 16. Juni 2022 in Berlin / Online	Ausbildung zum BSI IT-Grundschutz-Praktiker (DGI®)	Akademie der DGI Deutsche Gesellschaft für Informationssicherheit AG, Kurfürstendamm 57, 10707 Berlin Tel.: 030/31517389-10; Fax: 030/31517389-20
13. – 14. Juni 2022 in Berlin	Virtual Private Networks (VPN) – Konzeption und Realisierung	allskills Training Kastanienallee 53, 10119 Berlin Deutschland Tel.: 030/4492545; Fax: 030/44340435
13. – 17. Juni 2022 in Berlin	Microsoft Windows 11 / 10 Security und Deployment – Sicherheit	allskills Training Kastanienallee 53, 10119 Berlin Deutschland Tel.: 030/4492545; Fax: 030/44340435
20. Juni 2022 Online	Deep Dive IEC 62443-4-1 – Entwicklung sicherer Produkte für Industrie 4.0 & mehr	TÜV Informationstechnik GmbH Am TÜV 1. 45307 Essen Tel.: 0201/8999-404; Fax: 0201/8999-888 E-Mail: info@tuvit.de
20. – 24. Juni 2022 Berlin / Online	Ausbildung zum Lead Auditor ISO 27001 (DGI®)	Akademie der DGI Deutsche Gesellschaft für Informationssicherheit AG, Kurfürstendamm 57, 10707 Berlin Tel.: 030/31517389-10; Fax: 030/31517389-20
20. – 24 Juni 2022 München / Virtual Classroom	Informations-Sicherheitsbeauftragter / Chief Information Security Officer CERT/CISO	CBT Training & Consulting GmbH Elektrastr. 6a, 81925 München Tel.: 089/4576918-40; Fax: 089/4576918-25
20. – 23. Juni 2022 München / Virtual Classroom	IT-Forensik Spezialist CERT/ITFS	CBT Training & Consulting GmbH Elektrastr. 6a, 81925 München Tel.: 089/4576918-40; Fax: 089/4576918-25
20. – 24. Juni 2022 München / Virtual Classroom	EC-Council Certified Ethical Hacker CEH – EC-Council hat die aktuellsten Fortschritte auf dem Gebiet der Cybersicherheit in die Kursthemen aufgenommen.	CBT Training & Consulting GmbH Elektrastr. 6a, 81925 München Tel.: 089/4576918-40; Fax: 089/4576918-25
20. – 21. Juni 2022 in Berlin	E-Rechnungs-Gipfel 2022 – Die Pflicht zur E-Rechnung kommt!	Vereon AG Hauptstrasse 54, 8280 Kreuzlingen, CH Tel +41/71/67787-00
20. – 22. Juni 2022 in Berlin / Online	Ausbildung zum Kryptographie Security Expert (DGI®	Akademie der DGI Deutsche Gesellschaft für Informationssicherheit AG, Kurfürstendamm 57, 10707 Berlin Tel.: 030/31517389-10; Fax: 030/31517389-20
20. – 22. Juni 2022 Web-Seminar	IT-Grundschutz-Praktiker	isits AG International School of IT Security Huestr. 30, 44787 Bochum Tel.: 0234/927898-0; Fax: 0234/92/7898-20
20. – 22. Juni 2022 in Berlin	BSI: IT-Grundschutz-Berater	allskills Training Kastanienallee 53, 10119 Berlin Deutschland Tel.: 030/4492545; Fax: 030/44340435
22. – 23. Juni 2022 in Köln	Sicherheit in AWS-Cloud-Umgebungen	cirosec GmbH Ferdinand-Braun-Str.4 74074 Heilbronn Tel.: 07131/594550; Fax: 07131/59455-99 E-Mail: info@cirosec.de
27. – 29. Juni 2022 in Berlin / Online	Ausbildung zum ICS Security Manager gemäß IEC 62443, ISO 27001 und BSI IT-Grundschutz(DGI®)	Akademie der DGI Deutsche Gesellschaft für Informationssicherheit AG, Kurfürstendamm 57, 10707 Berlin Tel.: 030/31517389-10; Fax: 030/31517389-20

DATENSCHUTZ UND DATENSICHERHEIT

DuD – Datenschutz und Datensicherheit
Recht und Sicherheit in Informationsverarbeitung und Kommunikation
Ausgabe 6/2022, 46. Jahrgang | www.dud.de

Verlag
Springer Gabler | Springer Fachmedien Wiesbaden GmbH | Abraham-Lincoln-Straße 46 | 65189 Wiesbaden
Amtsgericht Wiesbaden, HRB 9754 | USt-IdNr. DE811148419
www.springer-gabler.de

Bezugsmöglichkeiten
Jährlich erscheinen 12 Hefte.
Jahresabonnement 2022 EUR 315,51
Jahresabonnement 2022 (Firmen, Institutionen und Bibliotheken) EUR 630,23
Jahresabonnement 2022 zum Vorzugspreis EUR 149,- gültig für persönliche Mitglieder der AwV (Arbeitsgemeinschaft für wirtschaftliche Verwaltung), des BvD (Berufsverband der Datenschutzbeauftragten Deutschlands e.V.), der DVD (Deutschen Vereinigung für Datenschutz e.V.), der DGRI (Deutsche Gesellschaft für Recht und Informatik), des FIfF (Forum Informatiker/Innen für Frieden und Gesellschaftliche Verantwortung e.V.), der GI (Gesellschaft für Informatik), für persönliche Mitglieder von TeleTrusT (Der IT-Sicherheitsverband Deutschlands). Der Vorzugspreis wird eingeräumt, wenn eine Bestätigung der Mitgliedschaft bzw. eine Studienbescheinigung vorgelegt wird.

Einzelheftpreis EUR 43,-

Alle Preise gelten zuzüglich Versandkosten. Alle Bezugspreise und Versandkosten unterliegen der Preisbindung.

Bezug durch den Buchhandel oder den Verlag. Abbestellungen müssen schriftlich spätestens 6 Wochen vor Ende des Bezugszeitraumes erfolgen. Im laufenden Jahrgang kann jeweils ein Sonderheft erscheinen, das nach Umfang berechnet und den Abonnenten im Erscheinungsjahr mit einem Nachlass von 25% des jeweiligen Ladenpreises geliefert wird. Bei Nichtgefallen kann das Sonderheft innerhalb einer Frist von 3 Wochen zurückgegeben werden.

Hinweise für Autoren
Bitte beachten Sie die ausführlichen Informationen unter www.dud.de. Manuskripte möglichst in maschinenlesbarer Form (Word-Datei) an den zuständigen Herausgeber (Report: Herr Reimer, Recht: Frau Mester oder Herr Buchner und Technik: Herr Fox) senden. Leserbriefe an die Herausgeber sind erwünscht, deren Publikation und eventuelle Kürzungen vorbehalten.

Geschäftsführer
Stefanie Burgmaier | Joachim Krieger | Juliane Ritt

Gesamtleitung Produktion
Ulrike Drechsler

Leiter Media Sales
Volker Hesedenz

Abonnentenverwaltung | Leserservice
Springer Customer Service Center GmbH
Haberstr. 7 | D-69126 Heidelberg
Telefon: (06221) 345-4303
Telefax: (06221) 345-4229
Montag bis Freitag, 8.00 Uhr bis 18.00 Uhr
E-Mail: springergabler-service@springer.com

Produktmanagement
Elke Janosch
Telefon: (030) 82 787-5367
Telefax: (030) 82 787-5365
E-Mail: elke.janosch@springer.com

Anzeigen
Anzeigenverkauf: Kerstin Feindler-Koch
Telefon: (0611) 7878-217
Telefax: (0611) 7878-78217
E-Mail: kerstin.feindler@springer.com

Anzeigendisposition: Petra Steffen-Munsberg
Telefon: (0611) 7878-164
Telefax: (0611) 7878-78164
E-Mail: petra.steffen-munsberg@springer.com

Es gilt die Anzeigenpreisliste vom 01.10.2018.

Produktion
Eva-Maria Krämer

Technische Redaktion
Oliver Reimer
Am Hohlstedter Weg 1a | 99441 Großschwabhausen
Telefon: (036454) 130040
Telefax: (036454) 130041
E-Mail: oliver.reimer@cmyk.one

Satz
Oliver Reimer | Großschwabhausen

Druck und Verarbeitung
Wilco | Amersfoort | Niederlande

Gedruckt auf säurefreiem und chlorarm gebleichtem Papier. | Printed in Germany

ISSN print 1614-0702

Dieser Ausgabe liegen Beilagen des Kunden Verlag Dr. Otto Schmidt aus Köln, bei. Wir bitten unsere Leser und Leserinnen um Beachtung.