genua.

Anomalie-Erkennung stärkt Datenschutz und Compliance

Bisherige IT-Security-Maßnahmen sind nicht mehr ausreichend. Die gestiegenen Anforderungen durch Datenschutz, Compliance und Cyber-Resilienz erfordern umfassendere Lösungen. Hier setzt eine Anomalie-Erkennung des Netzwerkverkehrs mit cognitix Threat Defender der genua GmbH an. Sie ermöglicht bessere und erweiterte Sicherheitskonzepte und wird zum Stand der Technik.

SecurITy made in Germany

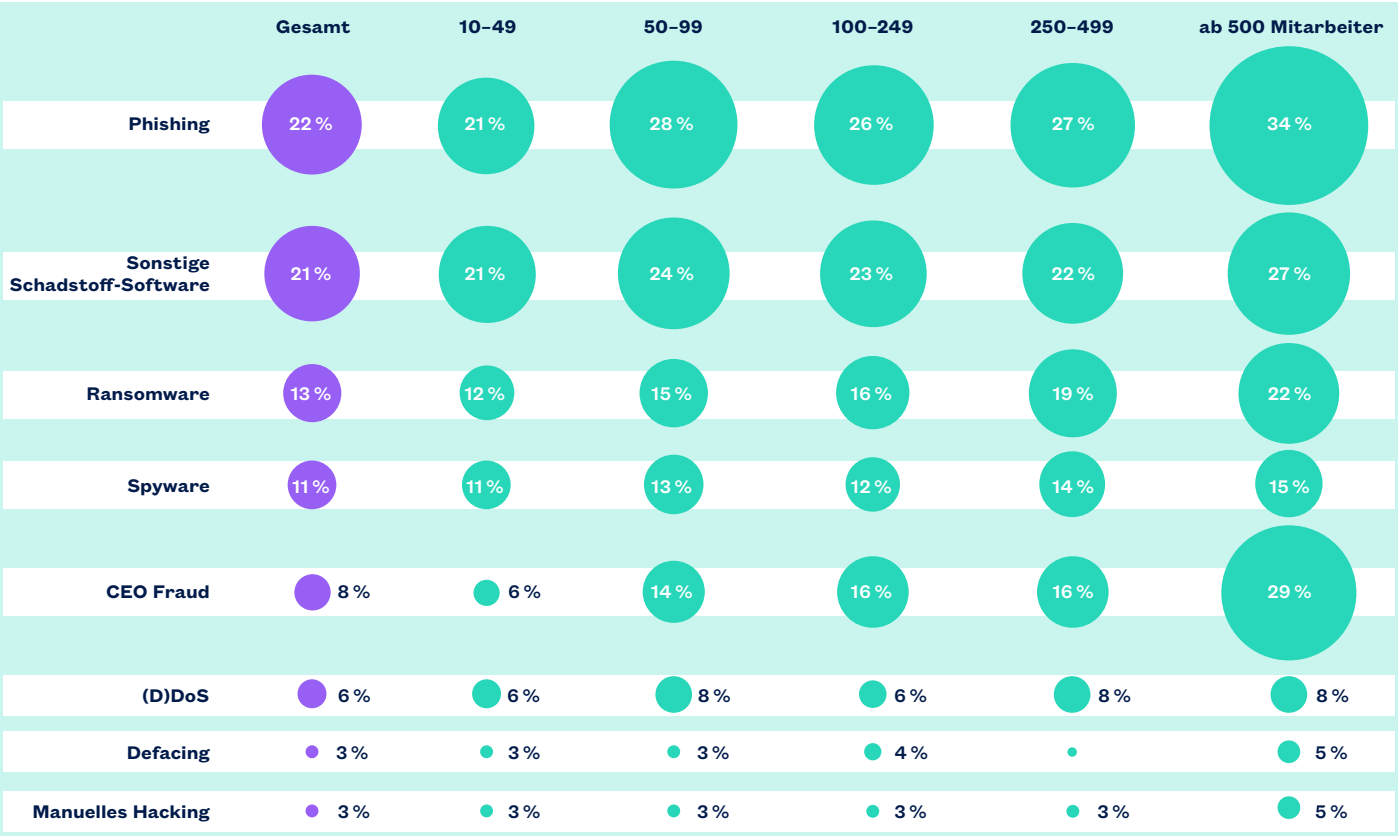
Inhalt.

1. Cyber-Angriffe werden erfolgreicher

Cyber-Angriffe werden erfolgreicher und bisherige Abwehrmaßnahmen verlieren durch immer intelligentere Angriffe an Wirksamkeit. Das Forschungsprojekt des Kriminologischen Forschungsinstituts Niedersachsen e.V. (KFN) ermittelte in einer repräsentativen Befragung von 5.000 Unternehmen, dass 65 Prozent der Befragten von mindestens einem Cyber-Angriff betroffen waren, 41 Prozent allein in den letzten zwölf Monaten (KFN 2020, „Cyberangriffe gegen Unternehmen“). Die Cyber-Angriffe waren erfolgreich, obwohl in diesen Unternehmen Schutzmaßnahmen vorhanden waren, wie aktuelle Antivirensoftware, regelmäßige Sicherheits-Updates oder Firewalls.

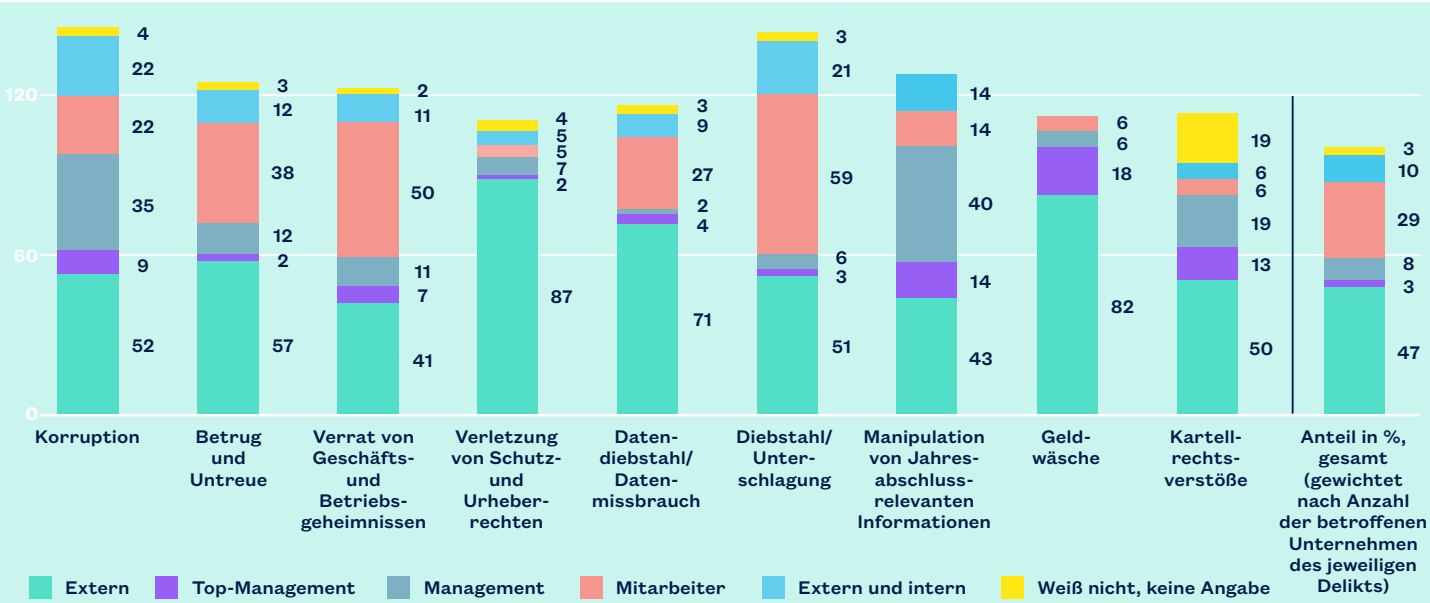
Viele der Sicherheitsvorfälle entstehen durch menschliche Schwächen und Datendiebstahl durch Mitarbeiter. Oft sind Mitarbeiter nur unbewusste Mittäter, indem sie auf Phishing-E-Mails reagieren, im Umgang mit Passwörtern ungenügende Sorgfalt walten lassen oder auf andere Art ermöglichen, dass Angreifer die Kontrolle über Accounts und/oder Geräte im Unternehmensnetzwerk erlangen können. So fordern gut gemachte Phishing-E-Mails mit falschen Angaben Mitarbeiter auf, Daten herunterzuladen oder Passwörter anzugeben.
Erfolgreiche Cyber-Angriffe können laut der KFN-Studie auch für kleine und mittlere Unternehmen bestandsgefährdende Kosten nach sich ziehen, worauf die große Spanne von bis zu zwei Millionen Euro hinweist. Zu den Angriffsarten, die die höchsten durchschnittlichen Kosten verursacht haben, zählen Ransomware-Angriffe, manuelles Hacking und (D) DoS-Angriffe.

Phishing gehörte zu den häufigsten Angriffsarten
(Betroffenheit nach Angriffstechnik und Unternehmensgröße in den letzten zwölf Monaten)



Quelle: KFN (2020): „Cyberangriffe gegen Unternehmen“

Verrat von Geschäfts- und Betriebsgeheimnissen:
Täter kommen vor allem aus dem eigenen Unternehmen (Cyber-Angriffe nach Täterherkunft; Anzahl der Unternehmen)



Quelle: KPMG „Wirtschaftskriminalität in Deutschland 2020“

2. Die Herausforderungen durch Compliance und Datenschutz

Unternehmen sehen das größte Risiko darin, von Datendiebstahl und Datenmissbrauch betroffen zu sein. Auch die Verletzung von Schutz- und Urheberrechten oder der Verrat von Geschäfts- und Betriebsgeheimnissen gilt als besonders risikobehaftet (KPMG-Studie „Wirtschaftskriminalität in Deutschland 2020“). Es ist in der Verantwortung von Geschäftsführern und Vorständen, die Compliance-Anforderungen in der IT einzuhalten (dazu zählen insbesondere Informationssicherheit, Verfügbarkeit, Datenaufbewahrung und Datenschutz).

So benennt Art. 5 der Datenschutz-Grundverordnung (DSGVO) Grundsätze, die bei der Verarbeitung personenbezogener Daten einzuhalten sind: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz; Zweckbindung; Datenminimierung; Richtigkeit; Speicherbegrenzung, Integrität und Vertraulichkeit.

In der DSGVO werden Verstöße gegen den Datenschutz mit Strafen von bis zu zwei Prozent des Konzernumsatzes sehr hoch angesetzt.

3. Das Ziel: Cyber-Resilienz

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) betont, dass ein vollständiger Schutz vor Cyber-Risiken nicht zu erreichen bzw. ein unrealistisches Ziel ist. Es gehe vielmehr darum, durch eine Risikoanalyse zwischen unternehmenskritischen Assets (den „Kronjuwelen“ des Unternehmens) und anderen Daten oder Systemen zu unterscheiden. Unternehmen sollten den größten Wert auf ausgefeilte Abwehrmechanismen legen, die so konzipiert sind, dass sie die wichtigsten Daten und Systeme des Unternehmens schützen (BSI/Allianz für Cyber-Sicherheit, „Management von Cyber-Risiken: Handbuch für Unternehmensvorstände und Aufsichtsräte“).

Das Ziel besteht darin, durch organisatorische und technische Maßnahmen eine Cyber-Resilienz zu erreichen.

Ein Unternehmen gewinnt dadurch die Fähigkeiten, auch bei einem erfolgreichen Cyber-Angriff weiterhin handlungsfähig zu sein. Resilienz ist laut BSI die Fähigkeit eines Systems, mit Veränderungen umgehen zu können. Resilienz bedeutet demnach die Widerstandsfähigkeit gegen Störungen jeder Art, Anpassungsfähigkeit an neue Bedingungen und eine flexible Reaktion auf Veränderungen mit dem Ziel, das System – z. B. einen Betrieb oder einen Prozess – aufrechtzuerhalten.

4. Ein neues Schutzniveau durch Anomalie-Erkennung

Durch die immer ausgefeilteren Angriffsszenarien und Angriffstechniken werden Cyber-Attacken immer effektiver im Datenstrom von z. B. HTTP, HTTPS, POP3 oder IMAP verschleiert. Die Kommunikation ist größtenteils verschlüsselt und schwer zu überprüfen. Ein Angriff und die Aktivität von Malware sind deshalb oft nicht auf den ersten Blick zu erkennen. So finden Schadprogramme trotz Firewall und Viren-Scanner einen Weg in das Unternehmensnetzwerk.

4.1 Monitoring der Netzkommunikation (IDS/IPS)

Das Monitoring des Netzwerkes ist eine Schutzmaßnahme, um die Netzwerkkommunikation zu überwachen und auf Auffälligkeiten zu untersuchen. Dafür haben sich Intrusion-Detection-Systeme (IDS) und Intrusion-Prevention-Systeme (IPS) etabliert. Sie werden bereits seit vielen Jahren eingesetzt.

Ein wesentlicher Nachteil von IDS und IPS ist, dass sie auf Auffälligkeiten im Datenstrom begrenzt sind. Nimmt bspw. eine beliebige Netzkomponente plötzlich Kontakt zu allen anderen Netzwerkkomponenten auf, ist der individuelle Datenstrom selbst nicht unbedingt auffällig und wird deshalb nicht detektiert. Das IDS überprüft nicht, ob diese Netzkomponente dazu berechtigt ist. Es überprüft auch nicht, ob dieses Verhalten für diese Netzkomponente ungewöhnlich ist. So können Angreifer Geräte im Netz übernehmen, ohne dass dies sofort auffällt.

Höchstes Schutzniveau durch Anomalie-Erkennung – mit der IT-Sicherheitsplattform cognitix Threat Defender.

4.2 Bisher getrennte Sicherheitsfunktionen zusammenführen

cognitix Threat Defender von genua schließt die Sicherheitslücke von IDS und IPS. Er überwacht den gesamten Netzwerkverkehr und analysiert auch das Verhalten der Netzkomponenten (Assets). cognitix Threat Defender richtet ein überwachtes sicheres Netzwerk ein, indem er Verhaltensmuster der Netzwerkgeräte erkennt (Anomalie-Erkennung) und definierten Regeln zuordnet. Dabei werden bisher getrennte Funktionen wie Netzwerkanalyse, Intrusion Detection, Asset Tracking und eine dynamische Policy Engine in einem System zusammengeführt.

4.3 Anomalie-Erkennung wird zum Stand der Technik

Die Cyber-Sicherheits-Empfehlung des BSI (BSI-CS 134) hebt die Anomalie-Erkennung als ein Mittel zum Schutz von Netzwerken besonders hervor: „Sie ermöglicht die Erkennung untypischen Verhaltens und somit neben technischen Fehlerzuständen und Fehlkonfigurationen auch die Detektion bisher unbekannter Angriffsformen auf solche Netze. Dies unterscheidet die Anomalie-Erkennung von anderen Maßnahmen, die auf der Erkennung bereits bekannter Angriffe beruhen."

Die Forderung nach einer Anomalie-Erkennung findet sich auch im Entwurf „IT-Sicherheitsgesetz 2.0" (IT-SiG 2.0). „Diese Systeme stellen eine effektive Maßnahme zur Begegnung von Cyber-Angriffen dar." Die Betreiber kritischer Infrastrukturen werden demnach erstmals zum Einsatz von Systemen zur „Angriffserkennung" verpflichtet IT-SiG 2.0 vom 07.05.2020).

5. Ein sich selbst überwachendes sicheres Netzwerk

Durch die transparente Integration in das Netzwerksegment analysiert cognitix Threat Defender den gesamten Netzwerkverkehr in diesem Segment rückwirkungsfrei, d. h. ohne Änderungen von IP-Adressen und mit nur minimalen Änderungen an der Infrastruktur. Dadurch wird der Netzwerkverkehr von allen Geräten im Netzwerksegment erkannt. Daraus wird automatisch die Asset-Datenbank gefüllt, die dann mit externen Inventory-Systemen abgeglichen werden kann. So können unbekannte oder unerwartete Netzwerkteilnehmer direkt gefunden werden. Außerdem wird auf diese Weise das gesamte Verhalten der Netzwerkteilnehmer analysiert und bestimmt. Das Echtzeit-Reporting über den Netzwerkverkehr sowie die Assets sorgen dabei für Einblicke und Erkenntnisse auch in die bisher dunklen Bereiche des Netzwerksegments.

Die Assets können dann nach Funktion und Aufgaben markiert werden, um eine bessere Übersicht im Netzwerk zu gewinnen. Außerdem ist dadurch die Trennung von Infrastruktur und Security klar geregelt. Die Netzwerkadministratoren können sich um die Infrastruktur, die Netzwerkteilnehmer und die Funktionen der Geräte kümmern. Die Security-Administratoren können die Sicherheitsbestimmungen für die Funktionen festlegen und bestimmen, auf welches Verhalten mit welcher Policy reagiert wird. Wenn das Gerät mehrere Funktionen hat, gelten mehrere Sicherheits-Policies. Diese greifen dann dynamisch ineinander: Wird einem Gerät eine neue Funktion zugeordnet, treten automatisch neue Sicherheitsbestimmungen für dieses Gerät in Kraft. Ändert sich das Verhalten des Geräts, wird dieses neue Verhalten nach den Vorgaben der Security-Experten erneut behandelt.

Damit findet eine dynamische und transparente Segmentierung des Netzwerkes auf Layer 7 im Netzwerk statt und nicht mehr nur am Übergang zu einem anderen Netzwerksegment. Welche Sicherheitsvorgaben für ein Gerät gelten, bestimmt sich also nicht mehr nach dem Netzwerkport oder dem Switch, an dem das Gerät eingesteckt ist. Wie ein Gerät mit den anderen Teilnehmern des gleichen Netzwerkes oder anderer Netzwerke kommunizieren darf, entscheidet sich nun anhand der Funktion und des Verhaltens.

6. Compliance durch Anomalie-Erkennung wirksam verbessern

Die Anomalie-Erkennung kann das Schutzniveau gegenüber zielgerichteten Schadprogrammen und mehrstufigen, schwer zu entdeckenden Angriffen deutlich verbessern. Dies unterstützt die Schutzmaßnahmen von der Business Continuity bis zur Förderung der Cyber-Resilienz.

6.1 Business Continuity absichern

Die unterbrechungsfreie Verfügbarkeit (Continuity) geschäftskritischer Prozesse ist für Unternehmen existenziell und muss deshalb durch präventive Maßnahmen und Notfallvorsorgepläne (Business Continuity Management) sichergestellt werden.

cognitix Threat Defender dient als Werkzeug der Netzwerkdiagnose dazu, Probleme frühzeitig zu erkennen und Vorhersagen für zukünftige Probleme/Hotspots zu treffen. So kann sich bspw. durch den Backup-Verkehr schleichend eine Überlastsituation im Netzwerk aufbauen. Diese Überlast kann unternehmenskritische Anwendungen stören oder zu Unterbrechungen führen. cognitix Threat Defender zeigt die Entwicklung des Traffics und liefert außerdem Informationen über die verursachenden Applikationen. Durch Regeln in cognitix Threat Defender kann Business-kritischer Traffic priorisiert und anderer Traffic in Extremsituationen oder zeitbasiert limitiert oder komplett unterbunden werden.

6.2 Sabotage verhindern

Sabotage, bspw. durch Überlastungen des Datennetzes, durch Auslastung der Internetanbindung mittels File Sharing oder durch eine große Zahl an Rechnern (DDoS-Attacke) oder durch gezielte Angriffe auf Steuerungssysteme von Produktionsunternehmen, hat häufig fatale Folgen wie Produktionsausfälle, Produktfehler oder Störungen in den Geschäftsprozessen.

Zu den typischen Sabotageangriffen zählen DoS-Attacken (Denial-of-Service) mit einer Vielzahl von gezielten Anfragen, um einzelne Komponenten des Datennetzes wie E-Mail-Server oder Citrix-Terminal-Server zu überlasten, zu blockieren und damit Ausfälle der Produktivität zu verursachen. cognitix Threat Defender kann hier als zusätzliche Schutzebene für die Server fungieren, indem nur eine bestimmte Anzahl von Verbindungen pro Absender zugelassen wird. Gleichzeitig wird von cognitix Threat Defender in Echtzeit erkannt, welche der Verbindungen im Netzwerk nicht dem Normalverhalten entsprechen. Diese werden gekennzeichnet und können manuell oder automatisch geblockt werden. Durch weitere Regeln lassen sich z. B. Zugriffsbeschränkungen für systemkritische File Server festlegen, sodass Zugriffe nur von bestimmten Rechnern aus möglich sind.

6.3 Verrat/Wirtschaftsspionage erkennen

Durch die Überwachung des Netzwerkverkehrs durch cognitix Threat Defender werden auffällige Zugriffe von Nutzern oder Geräten abseits „des Üblichen“ oder ungewöhnliche Datenströme zu externen Zielen erkannt. Dies kann ein möglichst unauffälliger kurzer Verkehr (Exfiltration einzelner „Erkenntnisse“) oder ein auf harmlose Datenraten beschränkter Datenstrom zur Exfiltration größerer Mengen von Daten sein. Möglich ist auch die Kombination der beiden Verhaltensmuster, und zwar sowohl gleichzeitig als auch nacheinander, indem auf das interne „Schnüffeln“ die Exfiltration folgt. Auch die Nutzung von nicht zugelassenen File Sharing-Diensten (Dropbox etc.), bisher nicht genutzten Cloud-Diensten oder Webmail-Providern kann ein Merkmal von Spionage sein.

6.4 Verstoß gegen Import-/Export-vorschriften vermeiden

Der Datenaustausch mit Ländern mit Exportbeschränkungen unterliegt strengen Reglementierungen. Dies gilt auch für Angestellte, die z. B. mit einem Laptop in solchen Ländern tätig sind. Verstöße gegen Import-/Exportvorschriften werden mit empfindlichen Strafen belegt und unterliegen der persönlichen Haftung des Geschäftsführers.

Mithilfe von cognitix Threat Defender kann der Datenaustausch mit Ländern mit Exportbeschränkungen auf „verdächtige“ Protokolle/Applikationen gefiltert werden. So können unproblematisch Protokolle wie NTP zur Zeitsynchronisation zugelassen werden, während Protokolle wie BitTorrent oder Traffic im Tor-Netzwerk blockiert werden.

Außerdem können externe Netzwerkzugriffe, abhängig vom Standort, unterschiedlich behandelt werden. So lässt sich der Zugriff eines Angestellten per VPN aus einem Land mit Exportbeschränkungen auf bestimmte Ressourcen unterbinden, mit extra Authentifizierungen versehen oder zumindest loggen. Bei einem Zugriff aus Ländern ohne Exportbeschränkungen kann der Zugriff durch das VPN dagegen uneingeschränkt erfolgen.

6.5 Die Cyber-Resilienz fördern

Um die Cyber-Resilienz zu fördern, können mithilfe von cognitix Threat Defender geschäftskritische Systeme und Prozesse besonders geschützt werden. So kann bspw. der Datenverkehr von Produktionsanlagen mit dem SAP-System als besonders schützenswerter unternehmenskritischer Prozess festgelegt werden, der nicht unterbrochen werden darf. Um das zu erreichen, werden die Produktionsanlagen und Arbeitsstationen als SAP-Devices markiert und für diese Assets Regeln definiert. Darin können z. B. Priorisierungen im Datenverkehr, eine maximale Anzahl von Anfragen oder zugelassene Kommunikationsprotokolle festgelegt werden. So können unerwünschte und problematische Zugriffe auf das SAP-System blockiert werden.

Durch das Markieren/Taggen von Netzwerkkomponenten lassen sich deren Security-Eigenschaften einzeln festlegen. So können Netzwerkbereiche anhand von Funktionen (und Verhalten) segmentiert und das Kommunikationsverhalten eingeschränkt werden. Dabei sind auch dynamische und überlappende Segmentierungen möglich, wie z. B. von SAP-Devices, die auch mit dem Druck-Server kommunizieren können. Ein weiterer gewünschter Effekt dieser Vorgehensweise ist die Trennung von Infrastruktur- und Security-Maßnahmen, um alle Security-Aktivitäten an einer Stelle zu bündeln.

7. Eine zusätzliche Kontrollschicht für den Datenschutz

Art. 5 der DSGVO benennt Grundsätze für die Verarbeitung personenbezogener Daten. Die DSGVO schreibt vor, dass Unternehmen die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nachweisen müssen („Rechenschaftspflicht"). Hier kann cognitix Threat Defender als ein Werkzeug zur Einhaltung der DSGVO genutzt werden.

Ein Verstoß gegen die Datenschutz-Grundverordnung (DSGVO) liegt bereits vor, wenn unberechtigte Personen auf Netzwerkbereiche zugreifen, in denen mit DSGVO-relevanten Daten gearbeitet wird. Der Datenschutz verpflichtet auch dazu, die Daten u. a. durch Backups gegen Verlust zu schützen.

Schutz vor unberechtigten Zugriffen
cognitix Threat Defender liefert die Instrumente, um die Rechtmäßigkeit und Transparenz bei der Verarbeitung personenbezogener Daten zu dokumentieren. So ist zu jeder Zeit transparent, welche Assets sich im Netzwerk befinden und wer mit wem kommuniziert. Durch Regeln kann der Zugriff auf Netzwerkbereiche, in denen personenbezogene Daten verarbeitet werden, auf berechtigte Devices beschränkt werden. Solche Zugriffe sollten generell im Rollen- und Berechtigungskonzept bzw. dessen Umsetzung im Rechtemanagement geregelt werden. So lassen sich unberechtigte Zugriffe auf File Shares der HR verhindern. cognitix Threat Defender übernimmt hier die Funktion einer zusätzlichen Kontrollebene auf der Netzwerkschicht.

Blocken von unsicheren Protokollen
Unverschlüsselte Protokolle zur Datenübertragung in Netzwerken bzw. zwischen Geräten mit personenbezogenen Daten (https vs. http, IMAPS vs. IMAP) stellen ein Sicherheitsrisiko dar. Ein Unterbinden dieser Protokolle und Kommunikationsarten verhindert ein Ausspähen der datenschutzrechtlich relevanten Daten durch Dritte.

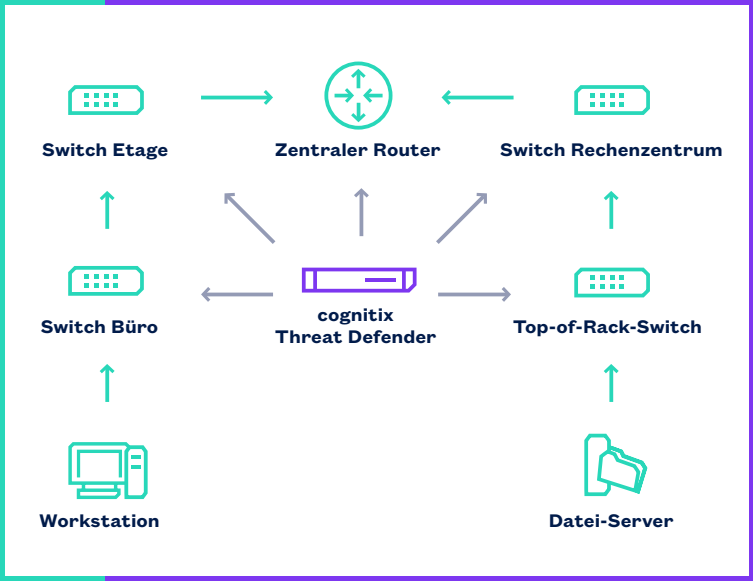
Schutz vor Datenverlust
Durch die Backup-Pflicht sollen Daten vor Verlust geschützt werden. Eine Datenhaltung abseits von offiziellen Daten-Servern mit eingerichtetem Backup ist also zu vermeiden (und meist ein Zeichen von Schatten-IT). cognitix Threat Defender kann das Netzwerk daraufhin überwachen, ob alle Dienste/Server, die Daten bereitstellen, regelmäßig mit dem Backup-System kommunizieren. Wenn ein solches System in einem definierten Zeitraum nicht mit dem Backup-System kommuniziert, wird ein Compliance-Alarm ausgelöst. Zusätzlich sollte zum Schutz der Backup-Daten geregelt werden, dass nur berechtigte Clients auf den Backup Server zugreifen dürfen.

Schutz der Datenintegrität
Der Schutz vor unberechtigten Zugriffen, das Unterbinden unsicherer Protokolle und der Schutz vor Datenverlust verhindern auch den Zugriff durch Verschlüsselungstrojaner.

8. Fazit

Ein vollständiger Schutz vor Cyber-Risiken ist nicht mehr zu erreichen. Durch immer intelligentere Angriffe finden Schadprogramme trotz Firewall und Viren-Scanner immer häufiger einen Weg in das Unternehmensnetzwerk. Das Ziel besteht deshalb darin, durch organisatorische und technische Maßnahmen eine Cyber-Resilienz zu erreichen und die wichtigsten Daten und Systeme des Unternehmens besonders zu schützen. cognitix Threat Defender unterstützt diese Maßnahmen und richtet ein sich selbst überwachendes sicheres Netzwerk ein. Durch die Anomalie-Erkennung wird die Netzwerksicherheit erhöht und ein neues Schutzniveau erreicht.

cognitix Threat Defender übernimmt die Funktion einer zusätzlichen Kontrollebene auf der Netzwerkschicht und verbessert so die Compliance. Unternehmen schützen sich wirkungsvoller vor Datendiebstahl und Datenmissbrauch. Auch die Verletzung von Schutz- und Urheberrechten oder der Verrat von Geschäfts- und Betriebsgeheimnissen werden effektiver unterbunden.



Der Einsatz von cognitix Threat Defender hilft außerdem, die Vorgaben der DSGVO besser einzuhalten. Das Gutachten einer Wirtschaftsprüfung bestätigt, dass cognitix Threat Defender das Einhalten der DSGVO in der EU unterstützt.

Weitere Informationen:

www.genua.de/threat-defender

https://youtu.be/iHs62Xh68uM

Über genua

Die genua GmbH versteht sich als Enabler der digitalen Transformation. Wir sichern sensible IT-Netzwerke im Public- und im Enterprise-Sektor, bei KRITIS-Organisationen und in der geheimschutzbetreuten Industrie mit hochsicheren und skalierbaren Cyber-Security-Lösungen. Dabei fokussiert sich die genua GmbH auf den umfassenden Schutz von Netzwerken, Kommunikation und interner Netzwerksicherheit für IT und OT. Das Lösungsspektrum umfasst Firewalls & Gateways, VPNs, Fernwartungssysteme, interne Netzwerksicherheit und Cloud Security sowie Remote-Access-Lösungen für mobile Mitarbeiter und Home Offices.

Die genua GmbH ist eine Tochtergesellschaft der Bundesdruckerei-Gruppe. Mit mehr als 350 Mitarbeitern entwickelt und produziert sie IT-Security-Lösungen ausschließlich in Deutschland. Seit der Unternehmensgründung 1992 belegen regelmäßige Zertifizierungen und Zulassungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) den hohen Sicherheits- und Qualitätsanspruch der Produkte. Zu den Kunden zählen u. a. Arvato Systems, BMW, die Bundeswehr, das THW sowie die Würth-Gruppe.

genua GmbH, Domagkstraße 7, 85551 Kirchheim bei München
T +49 89 991950-0, E info@genua.de, www.genua.de