TRUST IN GERMAN SICHERHEIT

G DATA

Whitepaper

Layered Security

G DATA CyberDefense AG | März 2017

Inhalt

Einführung

Angesichts der sich kontinuierlich weiterentwickelnden Bedrohungen für digitale Geschäftsprozesse ist nur ein umfassendes Sicherheitskonzept in der Lage, alle Phasen von Arbeitsabläufen ausreichend zu schützen. Layered Security beinhaltet herkömmliche Antiviren- und andere clientbasierte Schutzmechanismen, wehrt aber auch Risiken wie Ablaufunterbrechungen oder sogar vollständige Infrastrukturausfälle ab. In diesem Whitepaper werden verschiedene Arten von Risiken erörtert, denen sich digitale Unternehmen gegenübersehen, und die Schutzschichten diskutiert, die als Teil eines Layered Security Konzeptes implementiert werden sollten.

1. Risikokategorisierung

Die Aufgabe des IT-Administrators ist es sicherzustellen, dass die digitale Infrastruktur zuverlässige Produktivität ermöglicht. Vor diesem Hintergrund ist Sicherheitssoftware ein Mittel zum Zweck, aber keine endgültige Lösung. Der Administrator sollte die Risiken für die Infrastruktur kennen und die entsprechenden Lösungen aufspielen, um diese Risiken abzuwehren. Eine gute Möglichkeit, um einen Überblick über die Bedrohungen für digitale Geschäftsprozesse zu erhalten, ist, verschiedene Arten der Risikokategorisierung durchzuführen. Je nach Größe von Unternehmen und Infrastruktur kann und muss das Risikomanagement manchmal mittels eines Standardrahmens wie ISO 2700x, PCI DSS oder Common Criteria formalisiert werden. Auch wenn sie keine vollständige Sicherheits- und Risikomanagementstrategie ersetzen sollen, sind intentions-, element- und auswirkungsbasierte Ansätze ein Hilfsmittel, um Risiken aufzudecken und die Entwicklung angemessener Sicherheitskonzepte in die Wege zu leiten.

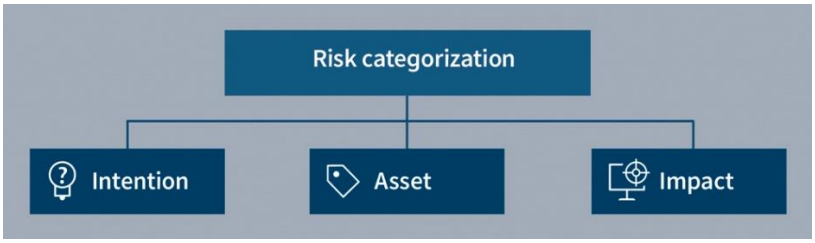

Abbildung 1: Risikokategorisierung

Nicht jeder Vorfall in einem Unternehmen ist das Ergebnis vorsätzlicher Planung eines Widersachers. Risiken anhand ihrer Intention zu kategorisieren, hat den Vorteil, dass die Aufmerksamkeit auf IT-Infrastrukturbedrohungen gelenkt wird, die ansonsten übersehen werden könnten. Die Natur ist beispielsweise einer der unberechenbarsten Faktoren: Gewitter oder extremer Niederschlag können, ganz ohne Vorsatz, riesigen Schaden an der IT-Infrastruktur verursachen. Es gibt eine Fülle anderer Risiken, die tägliche Abläufe unbeabsichtigt, aber erheblich beeinträchtigen können, zum Beispiel Fehler in Fremdkomponenten, falsche Konfigurationen oder die unabsichtliche Entfernung von Daten.

Die elementbezogene Analyse des Risikos ermöglicht eine andere Betrachtungsweise. An jedem digitalen Geschäftsprozess ist mindestens ein Element wie Hardware, Software, Daten oder Personal beteiligt. Jede dieser Kategorien kann in Unterkategorien aufgeschlüsselt werden, die ein Risiko darstellen. Bei Hardware sind die Risiken beispielsweise Verfügbarkeit, Schutz vor

Missbrauch und Leistung, wohingegen Datenrisiken hinsichtlich Backups, Datenschutz und Schutz vor unbefugtem Zugriff analysiert werden müssen.

Nicht immer lässt sich die potenzielle Auswirkung von Risikoszenarien berechnen. Nichtsdestotrotz müssen Was-wäre-wenn-Szenarien ausgewertet werden, um die Risiken mit der höchsten Beeinträchtigung zu ermitteln, die also vorrangig abgewehrt werden müssen. Die Beeinträchtigung hängt von der Art des Unternehmens, seinen Abläufen, seiner Infrastruktur und vielen weiteren Faktoren ab, kann aber normalerweise hinsichtlich Zeit, Kosten oder Vertrauen quantifiziert werden. Diese Faktoren schließen sich nicht gegenseitig aus. Beispielsweise kosten Vorfälle, die einen Infrastrukturausfall verursachen, nicht nur Zeit, sondern wirken sich aufgrund des Produktivitätsverlusts auch auf die Finanzen aus. Für Unternehmen, deren Prozesse Teil einer digitalen Wertschöpfungskette sind, wie beispielsweise ein Online-Shop, kann die potenzielle Beeinträchtigung durch Infrastrukturprobleme sogar noch größer sein. Und da Datenschutzgesetze wie HIPAA und HITECH immer stringenter werden, hat ein Verlust der Vertrauenswürdigkeit unter Umständen verheerende Folgen.

2. Layered Security Modell

Wie Risikoanalysen zeigen, gibt es vielfältige Risiken und Risikoarten. Typische Sicherheitssoftware hält jedoch nur die spezifische Bedrohung auf, für die sie entwickelt wurde. Um die Mitarbeiterproduktivität und die Infrastrukturverfügbarkeit zu gewährleisten, müssen die Lösungen eine Vielzahl möglicher Risiken abdecken. Moderne Lösungen dürfen sich nicht nur auf einen Schutztyp verlassen, sondern müssen aus mehreren kooperierenden Modulen bestehen, die eine sogenannte mehrschichtige Sicherheit ermöglichen.

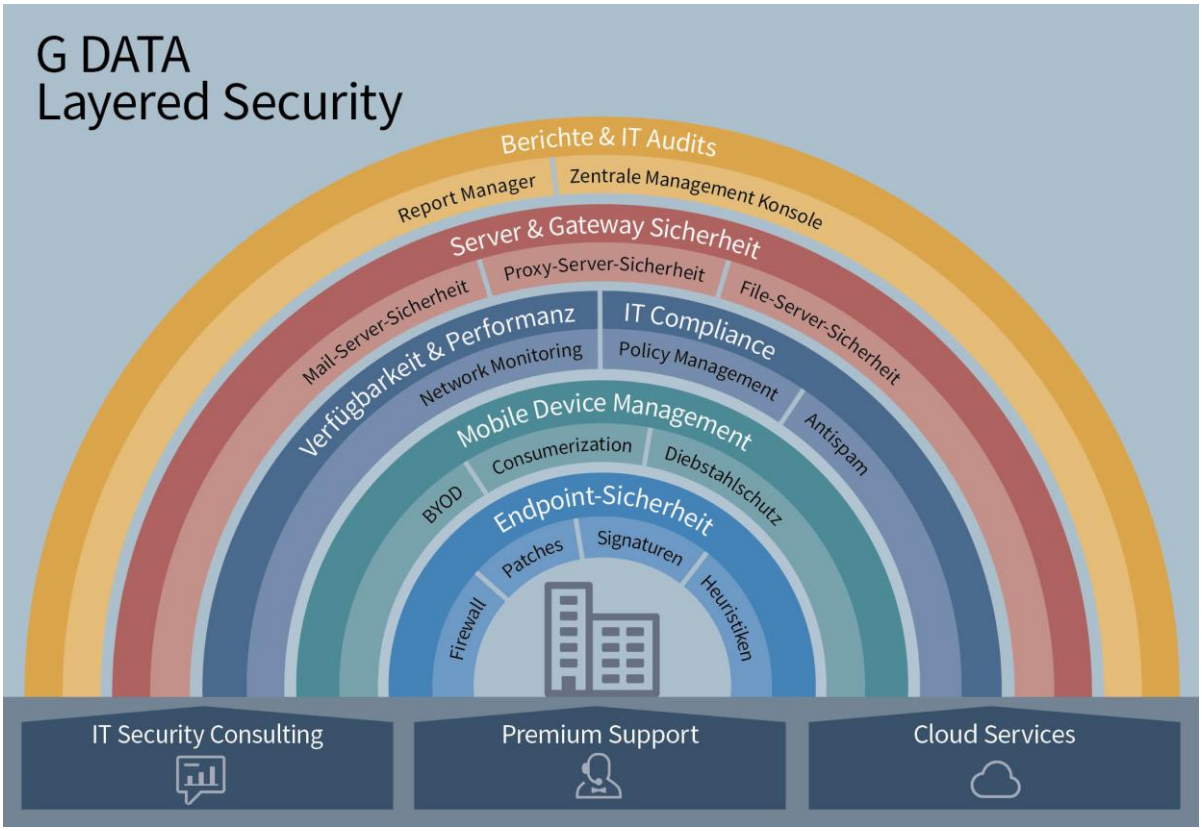

Abbildung 2: Layered Security Modell

Das Layered Security Modell ergänzt herkömmliche Sicherheitskomponenten um Technologien, die auch andere Arten von Risiken abwehren. Ein vollumfängliches, mehrschichtiges Konzept bietet nicht nur Sicherheit für Server und Endpoints, garantiert Verfügbarkeit, Performanz, Produktivität, Datensicherheit und Vertraulichkeit, sondern umfasst auch Services, die jede Schicht ergänzen.

2.1. Endpoint-Sicherheit

So wie die Layered Security für die Netzwerkinfrastruktur, besteht auch die Endpoint-Sicherheit aus mehreren Komponenten. Sie vereint sich gegenseitig ergänzende Module und verhindert, dass der Ausfall einer einzelnen Komponente das ganze System zum Erliegen bringt, wie es der Fall wäre, wenn man sich auf eine einzige Sicherheitstechnologie verlassen würde. Im Rahmen des Layered Security bietet sie eine optimale Kombination aus Schutzmodulen für Desktops und Laptops.

2.1.1. Firewall

Firewalls stoppen unbefugten Datenverkehr zum frühestmöglichen Zeitpunkt. In der Netzwerkschicht werden über das Internet an einen Endpunkt gesendete Pakete je nach festgelegten Netzwerksicherheitsregeln entweder durchgelassen oder gesperrt. Firewalls steuern den Datenverkehr auch in der Anwendungsschicht. Diese feinstufigere Kontrolle ermöglicht spezifische Sicherheitsrichtlinien je nach Anwendung, Port und Datenverkehr. Darüber hinaus sorgt dieser Ansatz für Sicherheit, auch wenn das Gerät außerhalb des Unternehmensnetzwerks verwendet wird. Verbindet sich ein Firmenlaptop mit einem anderen Netzwerk, stellt eine Client-Firewall sicher, dass das Sicherheitsniveau genau dem des Unternehmensnetzwerks entspricht.

2.1.2. Patches

In Betriebssystemen und Anwendungen werden regelmäßig Schwachstellen erkannt. Ihr Schweregrad reicht von Denial-of-Service-Angriffen über Fernzugriff bis hin zu Codeausführung per Fernzugriff. Auch wenn sich Softwareanbieter dieser Probleme bewusst sind und Patches zur Verfügung stellen, bedeutet dies nicht, dass sie umgehend aufgespielt werden. Im Zeitraum zwischen dem Erkennen einer Schwachstelle und dem Veröffentlichen bzw. Aufspielen eines Patches wird die Schwachstelle vielfach schon von Malware ausgenutzt. Daher sollte die betroffene Komponente schnellstmöglich nach der Patchveröffentlichung aktualisiert werden. Das Aufspielen von Patches ist eine wesentliche Voraussetzung, um Softwareschwachstellen dauerhaft abzuwehren. Es sorgt aber auch dafür, dass Anwendungen immer optimal funktionieren, indem beispielsweise Kompatibilitätsprobleme behoben oder Funktionen hinzugefügt oder erweitert werden. Allein aufgrund der hohen Anzahl von Patches und dem Test- bzw. Aufspielaufwand kann es Tage, ja sogar Wochen dauern, bis ein veröffentlichter Patch – falls überhaupt – implementiert wird. Daher wird unbedingt empfohlen, mit einer zentralen Patchverwaltungslösung zu arbeiten, die das Sammeln von Informationen, das Testen und das Aufspielen unterstützt.

2.1.3. Signaturen

Die signaturbasierte Erkennung ist eine der ältesten Methoden der Virenerkennung. Anhand statistischer Methoden werden Dateien mit Signaturen bekannter Malware verglichen, um Unregelmäßigkeiten aufzuspüren. Im Falle eines Treffers wird die Datei als bösartig gekennzeichnet und kann entweder gesperrt, gesäubert oder entfernt werden. Die signaturbasierte Erkennung ermöglicht die leistungsstarke Erkennung des Großteils bekannter Malware und bildet daher eine entscheidende Komponente des Layered Security Konzepts.

2.1.4. Heuristiken

Während bei der signaturbasierten Erkennung Signaturen aus bereits bekannten Malwaremustern erstellt werden müssen, basieren Heuristiken auf allgemeinen Merkmalen bösartiger Dateien. So können Heuristiken anhand der Dateikopfzeile oder anderer Codeteile beispielsweise sogar einen Virus erkennen, der so neu ist, dass es noch gar keine Signaturen für ihn gibt. Heuristiken stellen sicher, dass Viren entdeckt werden, bevor sie ausgeführt werden, auch wenn noch keine spezifischen Signaturen verfügbar sind.

Wie Heuristiken können auch verhaltensbasierte Technologien Malware stoppen, ohne auf vordefinierte Signaturen zurückgreifen zu müssen. Im Gegensatz zu Heuristiken sind sie jedoch auf die versuchten Aktionen der Malware angewiesen, statt auf datei- oder codebasierte Merkmale. Malware hat in der Regel eine bestimmte Verhaltensweise. Viele Arten fügen beispielsweise zusätzliche Einträge in die Registry oder kopieren sich an ganz bestimmte Speicherorte, um sich vor der Löschung zu schützen. Andere Arten laden einen bösartigen Schadteil von einem Online-Server herunter oder greifen auf verdächtige Bereiche im Arbeitsspeicher zu. Verhaltensbasierte Technologien erkennen typische Malware-Aktionen und stoppen den Verursacher, bevor er Schaden anrichten kann. Manche Implementierungen bieten breitgefächerte Verhaltenserkennung, während andere sich auf konkrete Einsatzszenarien wie Online-Banking oder Ransomware spezialisieren. Allen gemein ist, dass sie nicht auf vordefinierte Signaturen oder Merkmale angewiesen sind, so dass sie sogar bislang unbekannte Bedrohungen erkennen.

2.2. Mobile Device Management

Seit Smartphones und Tablets die Welt der Verbraucherelektronik im Sturm erobert haben, ist die Technologielandschaft erheblich komplizierter geworden. Durch Trends wie die Consumerizationder IT und BYOD (Bring Your Own Device; Einsatz privater Geräte für berufliche Zwecke hat eine Vielfalt von Geräten Einzug in Unternehmen gehalten. Es ist nun die Aufgabe des Administrators, den breitgefächerten Zugriff auf Ressourcen zuzulassen und gleichzeitig die Sicherheit zu gewährleisten. Das Mobile Device Management integriert diese Gerätevielfalt in bestehende Administrationsabläufe, um Geräteinstallation und -verwaltung möglichst effizient zu machen. Typische Komponenten sind Malware-Schutz, Diebstahlschutz und Geräterichtlinien.

2.3. Verfügbarkeit und Performanz

Eine IT-Infrastruktur muss sicher ausgeführt werden, doch das ist nicht der einzige zu berücksichtigende Faktor. Da die IT eine enorm wichtige Komponente der wirtschaftlichen Aktivität geworden ist, muss auch ihre Verfügbarkeit garantiert werden. Leistungsverlust und Ausfallzeiten haben eine unmittelbare Auswirkung auf die Betriebskontinuität. Im Unternehmen selbst brauchen die Mitarbeiter eine bei Bedarf immer verfügbare IT-Infrastruktur, um keine Produktivität einzubüßen. Nach außen hin verlassen sich Geschäftspartner und Kunden auf Web-Shops, Kommunikationssysteme, APIs und andere IT-Infrastruktur, so dass Ausfälle einen Umsatzverlust zur Folge haben. Um Verfügbarkeit und Leistung zu gewährleisten, umfasst Layered Security auch Überwachungskomponenten. Durch die Beobachtung historischer und aktueller Leistungsdaten und Verfügbarkeitsmetriken tragen Überwachungsfunktionen als Frühwarnsystem zur Verhinderung von Infrastrukturproblemen bei.

2.4. IT Compliance

E-Mail, Surfen im Internet und Software gehört alles zum normalen Geschäftsalltag. Fehlen jedoch Kontrollen, kann sich die unsachgemäße Nutzung von IT-Diensten negativ auf die Mitarbeiterproduktivität auswirken. Netzwerkweit gültige Richtlinien sollten dafür sorgen, dass der Internetzugriff im Allgemeinen wie auch konkrete Anwendungen nur den Benutzern zur Verfügung stehen, die sie auch tatsächlich brauchen. Es gibt auch äußere Einflüsse, allen voran Spam, die der Produktivität schaden. Spam macht mehr als die Hälfte des E-Mail-Datenverkehrs weltweit aus. Um zu verhindern, dass ungebetene Nachrichten die Infrastrukturleistung und die Mitarbeiterproduktivität beeinträchtigen, sollte auf Servern bzw. Clients ein Spamfilter installiert werden.

Der Schutz vertraulicher Informationen ist unumgänglich, um Handelsgeheimnisse, Verhandlungen und Produktentwicklungen zu schützen. Das Hauptmerkmal einer IT-Infrastruktur, also die effiziente Verteilung von Informationen, muss kontrolliert werden, damit keine vertraulichen Daten verloren gehen. Beispielsweise muss der Einsatz von USB-Sticks zur schnellen Übertragung von Dokumenten zwischen Computern in Umgebungen, in denen mit sensiblen Daten wie Finanztransaktionen oder Patientenakten gearbeitet wird, beschränkt werden. Ähnliches gilt für Software, damit vertrauliche Dateien nicht per E-Mail, Instant-Messaging und ähnlichen Tools verteilt werden. Daten können auch ganz ohne bösartigen Vorsatz verloren gehen. Der Ausfall einer Festplatte oder das versehentliche Löschen von Dateien kann sich äußerst negativ auf die Geschäftskontinuität auswirken. Insbesondere für Unternehmen, die Datenschutzauflagen wie HIPAA oder Sicherheitsrichtlinien-Rahmenwerken wie PCI DSS unterliegen, ist ein robustes Datensicherheits- und Backup-Konzept erforderlich, um Probleme zu vermeiden und im Notfall kurze Reaktions- und Wiederherstellungszeiten zu gewährleisten.

2.5. Server- und Gateway Sicherheit

Bevor Datenverkehr einen Endpoint erreicht, wird sein Inhalt oft von einem der Server verarbeitet, die sich üblicherweise im Unternehmensnetzwerk befinden, wie Mail- oder Proxy-Server. Aufgabe dieser Server ist es, unerwünschte Inhalte baldmöglichst auszufiltern. Beispielsweise können Mail-

Server wie Exchange, Sendmail oder Postfix mithilfe von Plug-ins E-Mails auf Spam oder Malware untersuchen, bevor sie an die Endpunkte zuggestellt werden. Analog schützen Web-Gatewayserver wie Squid den Web-Datenverkehr noch vor der Weiterleitung mithilfe von Antiviren-, Antispam- und Antiphishing-Technologie. Server- und Gateway Sicherheit ergänzt also die Firewall. Während Firewalls den Datenverkehr umfassend auf Basis vordefinierter Verbindungsregeln zulassen oder zurückweisen, analysiert Server- bzw. Gateway Sicherheit den Inhalt des Datenverkehrs. Außerdem sollten Dateiserver wie SAMBA geschützt werden, damit über sie keine Malware eines infizierten Clients im gesamten Netzwerk verteilt wird. Serversicherheit ist auch unerlässlich, wenn der Server Datenverkehr an Clients weiterleitet, die nicht durch ein Endpunktmodul geschützt sind. Verbinden sich nicht verwaltete Clients wie private Smartphones oder Gastgeräte mit dem Firmennetzwerk, sorgen serverbasierte Komponenten für deren Schutz. Server- und Gateway Sicherheitsmodule können ihrerseits mehrschichtig sein und beispielsweise cloud-, heuristik- oder signaturbasierte Komponenten umfassen.

2.6. Berichte und IT-Audits

Beim Abwehren von Infrastrukturrisiken wie Sicherheit, Verfügbarkeit und Leistung ist es nicht mit der Installation allein getan. Auch wenn viele der Komponenten einer Layered Security unabhängig voneinander ausgeführt werden, sollte der Administrator immer im Bilde sein und dafür sorgen, dass er stets auf die neuesten Informationen zugreifen kann. Daher definiert das Layered Security Modell Berichte und IT-Audits als unabhängige Schicht. Sie sollte dem Administrator ohne zu großen Aufwand anpassbare Berichte sowie Ereignis- und Alarmbenachrichtigungen bereitstellen. Der Administrator sollte auch in der Lage sein, schnell und einfach herauszufinden, welche Konfiguration für welche Netzwerkkomponenten gilt und um welche Module er sich dringend kümmern muss. Im Idealfall bietet eine integrierte Managementkonsole die Funktionalität, um alle Schichten zu konfigurieren, findet aber auch das richtige Verhältnis zwischen Konfigurierbarkeit und Benutzerfreundlichkeit.

2.7. Beratung, Support und Cloud-Services

Zusätzlich zu den einzelnen Schutzschichten des Modells umfasst Beratung, Support und Cloud-Services alle Schichten. Beispielsweise können cloudbasierte Technologien die Reputation verifizieren und die verschiedenen Sicherheitsschichten mit anderen nützlichen Informationen versorgen. Die Services umfassen auch Verwaltung und Konfiguration, beispielsweise für Unternehmen ohne eigene IT-Mitarbeiter. Anbieter verwalteter Dienste können Unternehmen jeder Größe mit Sicherheitslösungen versorgen und sich um Verwaltung und Konfiguration der Infrastruktur kümmern. Zu guter Letzt bieten Incident Response und Beratungsdienste Unternehmen Hilfestellung beim Einrichten und Pflegen von Sicherheitsrichtlinien und beim Abwickeln von Malwarevorfällen.

3. Auswahl einer Layered Security Lösung

Viele Netzwerke werden von Sicherheitslösungen geschützt, die aus sukzessiven und getrennt voneinander installierten Komponenten bestehen. Auch falls sie in ihrer Gesamtheit alle wichtigen

Sicherheitsschichten abdecken (was normalerweise nicht der Fall ist), arbeiten sie nur selten zusammen. Durch ein derart fragmentiertes, Layered Security Konzept wird die Infrastruktur anfälliger für Konfigurationsfehler (und die sich daraus ergebenden Sicherheitsprobleme) und erfordert mehr Zeit zur Konfiguration und Wartung. Empfohlen wird stattdessen, alle Sicherheitsschichten als integrierte Lösung mit allen notwendigen Komponenten und einer einheitlichen Verwaltungsschnittstelle zu implementieren. Die verschiedenen Schichten sollten die bestmögliche, ganzheitliche Sicherheit ohne Einbußen bei Leistung, Verwaltbarkeit oder Wirksamkeit bereitstellen. Darüber hinaus ist die Installation einer integrierten Lösung von einem einzelnen Anbieter – im Gegensatz zu Einzelkomponenten – oft mit einem finanziellen Vorteil verbunden.

Vor der Auswahl einer konkreten Lösung sollte der Administrator herausfinden, welche Teile der Infrastruktur geschützt werden müssen und welche Risiken gelten (siehe Kapitel 1). Sind Risikomanagementtools im Einsatz, können sie als Basis für die Auswahl einer Sicherheitslösung fungieren. Alternativ kann die Implementierung Layered Security auch mithilfe einer Liste wie SANS CIS Critical Security Controls, die empfohlene defensive Sicherheitskomponenten enthält, priorisiert und geplant werden[1]. Die zukünftige Lösung sollte nicht nur alle Risikoarten und Sicherheitsschichten abdecken, sondern auch die Verschiedenartigkeit der Endpunkte berücksichtigen. Sicherheitsschichten wie signaturbasierte Erkennung oder Heuristiken sollten für alle Endpunktarten (wie Windows-, Mac- und Linux-Clients und -Server) verfügbar sein. Mobile Device Management muss implementiert werden, damit auch Android- und iOS-Endpunkte sicher und in Übereinstimmung mit den Firmenrichtlinien eingesetzt werden. Durch die Einrichtung einer oder mehrerer server- oder infrastrukturbasierter Sicherheitsschichten wie beispielsweise die Netzwerküberwachung können viele Endpunkte und Aspekte wie Verfügbarkeit und Leistung auf einmal abgedeckt werden.

G DATA bietet Lösungen, die das gesamte Spektrum mehrschichtiger Sicherheitskomponenten abdecken und die vollständige Netzwerkinfrastruktur schützen, einschließlich einer Vielzahl verschiedener Endpoints sowie Mail-, Proxy- und Dateiserver. Durch das Kombinieren der Lösungen mit einer oder mehreren optionalen Modulen können die Lösungen an jedes Netzwerk angepasst werden, um Sicherheit, Verfügbarkeit, Leistung, Produktivität und Datensicherheit zu garantieren. Außerdem bietet G DATA verschiedene Services, von Supportvereinbarungen bis zu vollumfänglicher gehosteter Endpoint-Sicherheit. Aktuelle Informationen zu allen G DATA Business Solutions finden Sie unter www.gdata.de/business.

[1] Siehe https://www.sans.org/critical-security-controls.