avast

IT-Cybersecurity

Was KMUs von kritischen Infrastrukturen lernen können

Vorgaben kennen

Was das IT-Sicherheitsgesetz KRITIS vorschreibt

Maßnahmen ableiten

Wie Firmen von den gesetzlichen Vorgaben profitieren

Schutzwall errichten

Wie abgestimmte Sicherheits-lösungen den KMUs helfen

Datenblätter

Avast Business Hub
Avast Patchverwaltung
Avast Secure Internet Gateway

heise Business Services

Bild: Neelam279 / Pixabay

Editorial

Die Wasserversorgung bricht zusammen, das Stromnetz funktioniert nicht mehr, Krankenhäuser können ihre Patienten nicht behandeln: Wenn Hacker die IT-Systeme von kritischen Infrastrukturen (KRITIS) ins Visier nehmen, kann die öffentliche Ordnung zusammenbrechen. Damit ein solches Horrorszenario nicht Wirklichkeit wird, müssen KRITIS-Betreiber ihre IT umfassend schützen. Der Gesetzgeber verpflichtet sie mit strengen Vorgaben im IT-Sicherheitsgesetz dazu.

Aber nicht nur Wasserwerke, Kliniken oder Stromkonzerne mit Windkraftanlagen werden von Cyberkriminellen attackiert. Auch kleine und mittelgroße Unternehmen (KMUs) müssen sich gegen immer raffiniertere und immer neue Angriffe aus dem Internet wehren. Als „angespannt“ bezeichnet deshalb das Bundesamt für Sicherheit in der Informationstechnik die Lage der IT-Sicherheit in Deutschland.

Den KMUs fehlen allerdings häufig Budgets und Know-how, um ihre Infrastruktur ausreichend vor Hackerangriffen abzusichern. Trotzdem können sie von den Vorschriften lernen, die KRITIS erfüllen müssen, um ihre Daten und Ressourcen zu schützen. In diesem eBook zeigen wir, welche Bausteine aus dem IT-Sicherheitsgesetz auch für KMUs relevant sind und wie Avast-Lösungen helfen, diese ohne großen Aufwand umzusetzen.

Claudia Frickel
Journalistin

Inhalt

Wie sich kritische Infrastrukturen schützen müssen 3

Warum kritische Infrastrukturen besonders gefährdet sind 3

Was das IT-Sicherheitsgesetz KRITIS vorschreibt 4

Was ist ein ISMS und was gewährleistet es? 4

Brauchen auch andere Unternehmen ein ISMS? 5

Was KMUs aus den Vorgaben des IT-Grundschutzes ableiten können 6

Auch kleine und mittelgroße Unternehmen (KMUs) müssen sich schützen 7

IT-Sicherheit für KMUs in zehn Schritten 7

Mehr Cybersicherheit: die Vorteile für KMUs 8

Wie KMUs einen Schutzwall um ihre IT-Infrastruktur bauen 9

Ein automatisches Patch Management schützt vor Sicherheitslücken 9

Eine Firewall im Netzwerk 10

Sicherer Zugriff auf interne Anwendungen 10

Schutz vor infizierten Webseiten 11

Den Überblick behalten 12

Datenblätter 13

Avast Business Hub 13

Avast Patchverwaltung 15

Avast Secure Internet Gateway 17

Claudia Frickel schreibt seit 25 Jahren über alle Themen rund um Internet, IT, Computer und Smartphones. Die Journalistin beschäftigt sich mit allem, was dazugehört – von Sicherheit und Datenschutz über neue Trends und Technologien bis zur Nutzerfreundlichkeit. Im Zentrum stehen dabei sowohl die Perspektiven von Unternehmen als auch die Sicht der Anwender.

© 2021 Heise Medien

Alle Rechte vorbehalten. Nachdruck, digitale Verwendung jeder Art, Vervielfältigung nur mit schriftlicher Genehmigung der Redaktion.

Heise Medien GmbH & Co.KG
Abt. Heise Business Services
Hans-Pinsel-Straße 10b
85540 Haar bei München

Registergericht:
Amtsgericht Hannover HRA 26709

Persönlich haftende Gesellschafterin:
Heise Medien Geschäftsführung GmbH

Registergericht:
Amtsgericht Hannover, HRB 60405

Geschäftsführer:
Ansgar Heise, Dr. Alfons Schräder

Verantwortlich für den Inhalt:
Heise Business Services
Thomas Jannot, tj@heise.de

Layout: Oliver Eismann, stroemung GmbH

Haftung: Für den Fall, dass Beiträge oder Informationen unzutreffend oder fehlerhaft sind, haftet der Verlag nur beim Nachweis grober Fahrlässigkeit. Für Beiträge, die namentlich gekennzeichnet sind, ist der jeweilige Autor verantwortlich.

Abwehr von Cyberattacken und gesetzliche Vorgaben

Wie sich kritische Infrastrukturen schützen müssen

Ransomware, Schadprogramme, Datendiebstahl: Hacker haben zunehmend Unternehmen mit kritischen Infrastrukturen im Visier. Die müssen sich vor solchen Attacken besonders schützen und bekommen dafür strenge Auflagen – etwa die Implementierung eines ISMS wie dem BSI-Grundschutz. Doch welche genauen Vorgaben macht der Gesetzgeber?

Unternehmen, Behörden und Organisationen stehen unter ständigem Beschuss von Cyber-Kriminellen. Allein 322.000 neue Varianten von Schadprogrammen verzeichnet der Bericht „Die Lage der IT-Sicherheit in Deutschland 2020“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI) von 2019 bis 2020 – jeden Tag. Die Angreifer versuchen mit allen möglichen Mitteln, ihren Opfern zu schaden. Sie verschlüsseln Daten via Ransomware und wollen damit Geld erpressen. Sie stehlen Daten und legen mit Denial-of-Service-Attacken den Betrieb lahm. Oder sie verschaffen sich die Kontrolle über ein System.

Warum kritische Infrastrukturen besonders gefährdet sind

Besonders gefährlich ist die Situation für Betreiber kritischer Infrastrukturen (KRITIS). Bei Angriffen auf sie ist nicht nur die öffentliche Ordnung in Gefahr, auch Menschenleben können bedroht sein. Wenn beispielsweise der Strom nicht mehr geregelt fließt, fallen Ampeln aus und die Gefahr von Unfällen steigt.

2020 nahmen die Attacken auf KRITIS zu. Besonders stark war der Anstieg im Gesundheitswesen: 2019 hatten Hacker 16 Mal versucht, sich Zugriff auf Systeme in Krankenhäusern und anderen Einrichtungen zu verschaffen. 2020 passierte das laut Bundesregierung schon 43 Mal.

Mitunter haben die Angreifer Erfolg: Im September 2020 legten Kriminelle das Universitätsklinikum Düsseldorf wochenlang teilweise lahm. Sie hatten eine Sicherheitslücke in VPN-Lösungen von Citrix ausgenutzt. Einige Patienten mussten bei Rettungseinsätzen abgewiesen und an andere Krankenhäusern verwiesen werden, eine Frau starb während des dadurch längeren Transportweges.

Ernst hätte die Lage auch in Florida werden können. Im Februar 2021 verschaffte sich ein Hacker Zugriff auf den Zentralrechner eines Wasserwerks. Er nutzte dazu ein ungenügend geschütztes Tool zur Fernsteuerung. Dann erhöhte er den Anteil von Natriumhydroxid im Wasser auf einen gefährlichen Wert. Ein Mitarbeiter entdeckte die Manipulation zufällig.

Was sind kritische Infrastrukturen?

Kritische Infrastrukturen (KRITIS) sind laut BSI „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“ Dazu zählen **Energie- und Wasserversorger**, **Ernährung und Lebensmittelhandel**, **IT und Telekommunikation**, **Gesundheitswesen**, **Banken und Versicherungen** sowie **Transport- und Verkehrsunternehmen**.

Bild: Petovarga / Bigstock

Somit ist es wenig verwunderlich, dass KRITIS-Betreiber Cyberangriffe für das größte Sicherheitsrisiko halten, so eine Umfrage von Microsoft. Knapp dahinter auf Platz 2: das Fehlverhalten von Mitarbeitern.

Die Sicherheit ihrer IT-Systeme ist für kritische Infrastrukturen ebenso entscheidend wie für jedes andere Unternehmen. Aber KRITIS-Betreiber sind gezwungen, bestimmte Anforderungen zu erfüllen – das verlangt das BSI per Gesetz.

Was das IT-Sicherheitsgesetz KRITIS vorschreibt

Das IT-Sicherheitsgesetz verpflichtet KRITIS-Unternehmen, „die für die Erbringung ihrer wichtigen Dienste erforderliche IT nach dem Stand der Technik angemessen abzusichern." Je nach Branche müssen sie Standards mindestens erreichen. Andernfalls drohen Strafen bis zu 100.000 Euro. Zu den Vorgaben gehören unter anderem

- eine Meldepflicht bei Stör- und Sicherheitsvorfällen in der IT,
- ein regelmäßiges Audit mit Nachweis über die IT-Sicherheit (spätestens alle zwei Jahre),
- ein Business-Continuity-Management für den Ernstfall,
- die Einführung eines Informationssicherheits-Management-Systems (ISMS).

Was ist ein ISMS und was gewährleistet es?

Ein ISMS beschreibt alle Prozesse, Verfahren und Regeln in einem Unternehmen, die die Informationssicherheit dauerhaft definieren, steuern, kontrollieren, aufrechterhalten und verbessern. Dahinter steht ein ganzheitlicher und systematischer Ansatz: Es geht dabei nicht nur um die IT-Architektur selbst, sondern auch darum, Workflows und die Organisation im Hinblick auf die Sicherheit zu optimieren. Ein solches System hat einen Top-Down-Ansatz – alle Prozesse müssen mit der Unternehmensleitung starten.

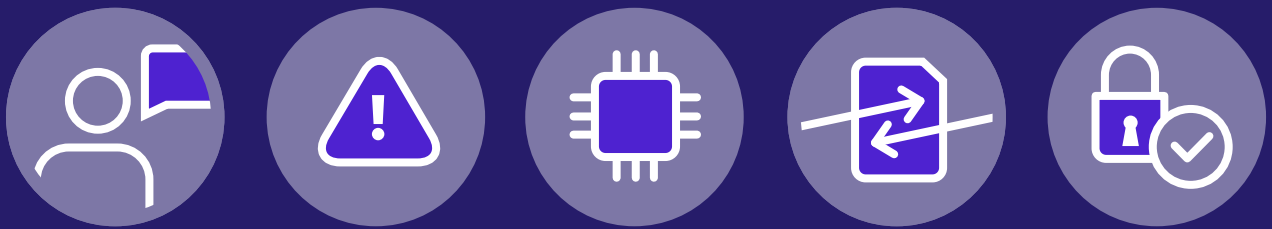
Ein ISMS gewährleistet unter anderem, dass

- Unternehmen eine Risikobewertung für ihre zentralen Prozesse vornehmen,
- Sicherheitsrichtlinien für den Umgang mit der IT-Infrastruktur festgelegt werden,
- aktuelles Wissen über Informationssicherheit vorhanden ist,
- Mitarbeiter in Bezug auf IT-Sicherheit qualifiziert sind und fortgebildet werden,
- die Informationssicherheit an die aktuelle Lage angepasst wird.

Das IT-Sicherheitsgesetz schreibt zudem vor, dass KRITIS-Betreiber ein zertifiziertes ISMS einführen. Meist erfolgt die Umsetzung mit der internationalen Norm ISO/IEC 27001 oder auf Grundlage des IT-Grundschutzes des BSI.

Anforderungen an KRITIS

Die Maßnahmen für eine offene Risikokommunikation lassen sich in fünf Stufen gliedern.



Kontaktstelle benennen

IT-Störungen melden

Stand der Technik umsetzen

Präventionsmaßnahmen und Reaktionspläne ausarbeiten

Absicherung prüfen lassen

Grafik: Eismann / stroemung GmbH

Die beiden Ansätze sind ähnlich: Sie betrachten den ISMS-Prozess jeweils als Zyklus in mehreren Phasen, die sich wiederholen – von der Planung und Konzeption über die Implementierung bis zur Erfolgskontrolle und der stetigen Optimierung.

Aber es gibt auch Unterschiede, vor allem in der konkreten Durchführung. ISO 27001 erfordert eine umfassende und aufwendige Risikoanalyse für alle Prozesse und Assets. Die Weisungen sind allgemeiner und lassen sich flexibler anpassen. Eine Risikoanalyse ist beim IT-Grundschutz dagegen nur bei Systemen mit erhöhtem Schutzbedarf notwendig. Das Konzept geht davon aus, dass bei den meisten typischen Anwendungen, Applikationen und Prozessen Standardmethoden ausreichend sind. Dafür müssen sich Unternehmen bei der Umsetzung der Vorgaben an konkrete Maßnahmen halten.

Brauchen auch andere Unternehmen ein ISMS?

Ein zentrales Informationssicherheits-Management-System ist nur für KRITIS-Betreiber verpflichtend. Es gewährleistet, dass sie ihre Infrastruktur vor Cyberangriffen schützen und die IT immer auf dem aktuellen Stand der Technik sind. Doch jedes Unternehmen kann ein ISMS etwa mit dem BSI-Grundschutz implementieren, um die IT-Sicherheit zu erhöhen. Für kleine und mittelgroße Unternehmen ist der Aufwand dafür allerdings oft zu hoch. Doch sie können von den Vorgaben, Bausteinen und Methoden lernen, um das eigene Schutzniveau zu erhöhen.

Millionen Menschen arbeiten dauerhaft oder häufig im Homeoffice, greifen über die Cloud auf das Firmennetzwerk zu und nutzen externe Kollaborations-Tools. Jede Menge Angriffsfläche für Cyber-Kriminelle.

Bild: Pheelings Media / Bigstock

Der IT-Grundschutz des BSI

Der IT-Grundschutz des BSI hat das Ziel, „das Niveau der Informationssicherheit in einer Institution anzuheben und aufrechtzuerhalten“, wie es bei der Behörde heißt. Er verfolgt „einen ganzheitlichen Ansatz zur Informationssicherheit: Neben technischen Aspekten werden auch infrastrukturelle, organisatorische und personelle Themen betrachtet. Er ermöglicht es, durch ein systematisches Vorgehen notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen.“

Der Grundschutz ist eine modular aufgebaute Sammlung von Methoden, Katalogen, Empfehlungen, Anforderungen und Standards. Im 810 Seiten umfassenden IT-Grundschutz-Kompendium finden sich unterschiedliche Bausteine. Sie sind in fünf sogenannte Schichten aufgeteilt:

Schicht 1 umfasst alle übergreifenden Aspekte der IT-Sicherheit, etwa Personal, Datensicherungskonzept und Outsourcing.

Schicht 2 betrifft baulich-technische Gegebenheiten, wie Gebäude, Serverräume oder Homeoffice-Plätze.

Schicht 3 dreht sich um die einzelnen IT-Systeme, also Server, Clients, Telefonanlagen, Notebooks und Smartphones.

Schicht 4 beschäftigt sich mit der Vernetzung der IT-Systeme. Es geht beispielsweise um WLAN sowie Netz- und Systemmanagement.

Schicht 5 befasst sich mit den Anwendungen selbst, etwa Datenbanken, E-Mail, Webserver und branchenspezifischen Programmen.

Informationssicherheit gewährleisten

Was KMUs aus den Vorgaben des IT-Grundschutzes ableiten können

Attacken aus dem Internet gefährden kleine und mittlere Unternehmen ebenso wie Konzerne und KRITIS-Betreiber. Der IT-Grundschutz enthält auch für die KMUs hilfreiche Bausteine zum Schutz ihrer Daten und Ressourcen. Aber sie haben oft nicht die Ressourcen, die detaillierten Vorgaben umzusetzen. Von den Leitlinien lernen können sie trotzdem.

Beinahe die Hälfte aller Unternehmen in Deutschland verzeichnete im Jahr 2019 Hacker-Angriffe, meldet der DsiN-Praxisreport Mittelstand 2020. Auch kleine und mittelgroße Unternehmen sind betroffen: 70 Prozent der deutschen KMUs vermelden, dass die Attacken zugenommen hätten, so der VMware Threat Report zu Cybersicherheit.

Das Problem: Anders als große Unternehmen fehlen diesen Betrieben oft die Budgets und die internen Ressourcen, um Sicherheitsstandards zu gewährleisten. Das wissen leider auch die Kriminellen und zielen deshalb bewusst auf die kleineren Firmen ab. Denn auch dort können sie sensible Daten abgreifen oder die Systeme über Ransomware verschlüsseln, um Lösegeld zu erpressen. Verschärft hat sich die Bedrohungslage durch die Corona-Pandemie, wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) bei der Vorstellung seines Berichts zur Lage der IT-Sicherheit in Deutschland 2020 warnte.

Unternehmen haben in der Krise die Digitalisierung vorangetrieben. Mitarbeiter arbeiten dauerhaft oder häufig im Homeoffice, greifen über die Cloud auf das Unternehmensnetzwerk zu und kommunizieren mithilfe externer Kollaborations-Tools wie Microsoft Teams mit Kollegen. Ein Bring-your-own-Device gilt oft als normal – Beschäftigte arbeiten dann etwa mit dem eigenen Laptop. Eine Kehrtwende zur alten Arbeitswelt wird es wohl nicht geben: 78 Prozent der Firmen gehen davon aus, dass der Übergang zu Remote Work dauerhaft sein wird, so eine Umfrage von PwC unter 700 Führungskräften.

Jede Menge Angriffsfläche für die Täter. Sie passen sich an – und nutzen neue Schwachstellen aus, wie es im Cyber Threatscape Report von Accenture heißt. Das Beratungsunternehmen warnt davor, dass Cyberangriffe in Zukunft deutlich häufiger vorkommen.

„Wenn wir weiterhin von der Digitalisierung profitieren wollen, dann dürfen wir es Angreifern nicht zu leicht machen“, so BSI-Präsident Arne Schönbohm. Trotzdem reagieren viele Firmen gar nicht oder nur zaghaft auf die Bedrohungen. Ein Viertel von ihnen hat laut dem „DsiN-Praxisreport Mittelstand“ keine Datensicherungen, 15 Prozent sind sich nicht darüber bewusst, dass ihre Software Schwachstellen hat, und 32 Prozent sagen, sie würden entweder nicht angegriffen – oder sie würden Attacken gar nicht identifizieren.

Cyber-Sicherheit in Deutschland

– eine Umfrage

73%

73 % der Unternehmen gaben an, sie hätten in den letzten zwölf Monaten ein Datenleck erlitten. Im Durchschnitt hat ein Unternehmen in diesem Zeitraum zwei Sicherheitsverletzungen erlitten.

82%

82 % der Unternehmen gaben an, die Angriffe seien ausgereifter geworden.

Bild: Aurielaki / Bigstock

Auch kleine und mittelgroße Unternehmen (KMUs) müssen sich schützen

Der Schutz ihrer IT-Sicherheit ist für KMUs deshalb ebenso essenziell wie für große Unternehmen und KRITIS-Betreiber. Die Implementierung eines ISMS über den IT-Grundschutz oder ISO 27001 stellt sie allerdings oft vor große Herausforderungen: Die Anforderungen sind komplex, die Umsetzung sprengt den zeitlich leistbaren Aufwand.

Aber KMUs können ihre IT und Infrastruktur umfassend schützen, ohne sich an die strengen Regularien halten oder sich zertifizieren lassen zu müssen. Aus dem IT-Grundschutz lassen sich Maßnahmen ableiten, die auch kleine und mittelgroße Unternehmen gut umsetzen können. Ein guter Informationsschutz und die grundlegende Absicherung der IT sind schon mit verhältnismäßig einfachen Mitteln zu erreichen.

IT-Sicherheit für KMUs in zehn Schritten

Der IT-Grundschutz des BSI enthält hilfreiche Ansätze, an denen sich kleine und mittelgroße Unternehmen orientieren können. Folgende zehn Schritte sind dabei essenziell:

1. Leitlinien erstellen und Sicherheitsbeauftragten ernennen

Unternehmen sollten ein Konzept für die IT-Sicherheit erstellen, das von der Führungsebene unterschrieben ist. Darin sind alle Maßnahmen dokumentiert. Es wird regelmäßig aktualisiert und überprüft. Ein Mitarbeiter sollte als Beauftragter ernannt werden, er braucht entsprechende zeitliche und finanzielle Ressourcen.

2. Mitarbeiter sensibilisieren und schulen

Die Beschäftigten müssen wissen, wie wichtig IT-Sicherheit ist, und sie müssen über bekannte oder neue Bedrohungen informiert werden – etwa zu den Gefahren, die durch Phishing oder den Download von Dateien entstehen.

3. IT-Systeme sicher konfigurieren

Nur notwendige Programme und Dienste sollten aktiviert sein. Die Rechte verschiedener Nutzer sind über Rollen definiert. Auch der Zugriff auf bestimmte Daten oder Funktionen sowie der Download von Apps ist für unterschiedliche Anwender geregelt.

4. Unternehmensnetzwerke und Schnittstellen absichern

Jeder Zugriff von außen auf das Unternehmensnetzwerk darf nur über eine Firewall möglich sein. Sie kann mögliche Angriffe abwehren. Der Schutzwall muss überwacht und die Regeln auf dem neuesten Stand gehalten werden. Sicherheitsrelevante Vorfälle müssen protokolliert und die Protokolle ausgewertet werden. Auf allen Servern und Netzwerkgeräten sollten nur die nötigen Dienste aktiviert sein.

5. Schwachstellen identifizieren und vor Schad-Software schützen

Antivirenscanner spüren Viren, Trojaner, Ransomware und andere Schad-Software auf und blocken sie. Der Virenschutz muss ständig aktualisiert werden. Betriebssysteme und Software müssen kontinuierlich gepatcht und alle Updates umgehend eingespielt werden, damit Angreifer Schwachstellen nicht ausnutzen können. Ansonsten können sie in die Systeme eindringen.

6. E-Mails und Internet sicher nutzen

Browser und E-Mail-Clients müssen auf dem neuesten Stand und sicher konfiguriert sein. E-Mails werden idealerweise verschlüsselt übertragen. Gefahren durch mit Malware infizierte E-Mails oder Webseiten müssen gebannt werden.

7. Sichere Passwörter und Zugangsdaten verwenden

Alle Hersteller-Passwörter müssen geändert werden. Es sollte eine Passwort-Richtlinie mit Mindestanforderungen geben (beispielsweise 8 Zeichen und mehr; Ziffern, Buchstaben und Sonderzeichen müssen enthalten sein usw.). Hilfreich ist eine Zwei-Faktor-Authentifizierung.

8. Alle Endgeräte schützen

Wenn Mitarbeiter Notebooks oder betriebliche Smartphones nutzen oder im Homeoffice arbeiten, müssen auch diese Geräte via Firewall und Virenschutz-Software abgesichert sein. Hilfreich ist eine Liste aller Endgeräte, die Schutz benötigen – dazu gehören auch Drucker, Server und Workstations. Daten müssen sicher über die Cloud übertragen und Kommunikationsdienste verschlüsselt benutzt werden.

9. Daten sichern und für den Notfall vorsorgen

Es sollten regelmäßig Backups aller Unternehmensdaten erstellt und diese sicher aufbewahrt werden. Außerdem sollte es Notfallpläne und Alternativlösungen für den Schadensfall geben.

10. Die Einhaltung von Compliance sicherstellen

KMUs müssen gewährleisten, dass alle IT-Assets in einem Inventar erfasst sind und ihr Schutzbedarf definiert ist. Es muss regelmäßig geprüft werden, ob alle im jeweiligen Betrieb geltenden Compliance-Anforderungen eingehalten werden.

Bild: Aurielaki / Bigstock

Mehr Cybersicherheit: die Vorteile für KMUs

Ein ganzheitlicher Sicherheitsansatz befasst sich sowohl mit Themen wie der Schulung der Mitarbeiter oder der Sicherstellung der Compliance als auch mit ganz konkreten Maßnahmen zum Schutz der IT. Dazu gehören Netzwerksicherung, Backups oder Endgeräteschutz. Externe Sicherheitslösungen helfen dabei, diese zu gewährleisten.

Kleine und mittelgroße Unternehmen, die ihre IT-Infrastruktur schützen, profitieren davon mehrfach:

- **Sie mindern die Risiken** etwa von Datenlecks, Datendiebstahl, Ransomware-Angriffen oder Sicherheitslücken durch ungepatchte Software.
- **Sie minimieren die IT- und Sicherheitskosten:** Eine verbesserte Sicherheit verringert den Zeit- und Kostenaufwand, der zur Schließung ausgenutzter Sicherheitslücken notwendig wäre. Laut einer IBM-Studie liegen die durchschnittlichen konsolidierten Gesamtkosten eines Datenlecks bei 3,86 Millionen US-Dollar. Auch Downtimes sind teuer.
- **Sie haben mehr Überblick über die eigene IT-Umgebung:** Sicherheitstools liefern transparente Informationen zur Firmen-IT-Infrastruktur.
- **Sie bleiben agiler:** Nur wenn Unternehmen ihre Assets und Infrastruktur schützen, können sie auf Anforderungen des Marktes reagieren.

Nicht zuletzt sind KMUs mit geschützten IT-Systemen und modernen Sicherheitslösungen auf die Zukunft vorbereitet – auch dann, wenn mehr Mitarbeiter remote arbeiten, sich die Schadprogramme wandeln oder die Hacker neue Methoden anwenden.

Mitarbeiter müssen wissen, wie wichtig IT-Sicherheit ist, und sie müssen ständig über Bedrohungen informiert werden. Schulungen sind nur ein erster Schritt.

Externe Sicherheitslösungen

Wie KMUs einen Schutzwall um ihre IT-Infrastruktur bauen

Netzwerke absichern, Patches einspielen, sicherer Zugriff auf das Internet und Unternehmensdaten: Speziell auf sie ausgerichtete Sicherheitslösungen helfen kleinen und mittelgroßen Unternehmen, wichtige Bausteine der IT-Sicherheit umzusetzen. Die Abschottung erfolgt automatisiert, das verringert den Aufwand.

Cyber-Kriminelle versuchen, jede Lücke auszunutzen, die sich ihnen bietet. Anfang März stellte Microsoft Security-Patches für eine Schwachstelle in seinem E-Mail-System Exchange bereit. Aber da war es schon zu spät: Angreifer hatten die Schwachstelle laut Microsoft bereits ausgenutzt und Ransomware auf Systemen von Firmen installiert.

Den Sicherheits-Patch müssen Firmen, die Exchange nutzen, allerdings selbst installieren. Acht Tage nach Veröffentlichung gab es weltweit 80.000 Exchange-Server, auf denen es nicht aufgespielt war, so eine Analyse von Palo Alto Networks.

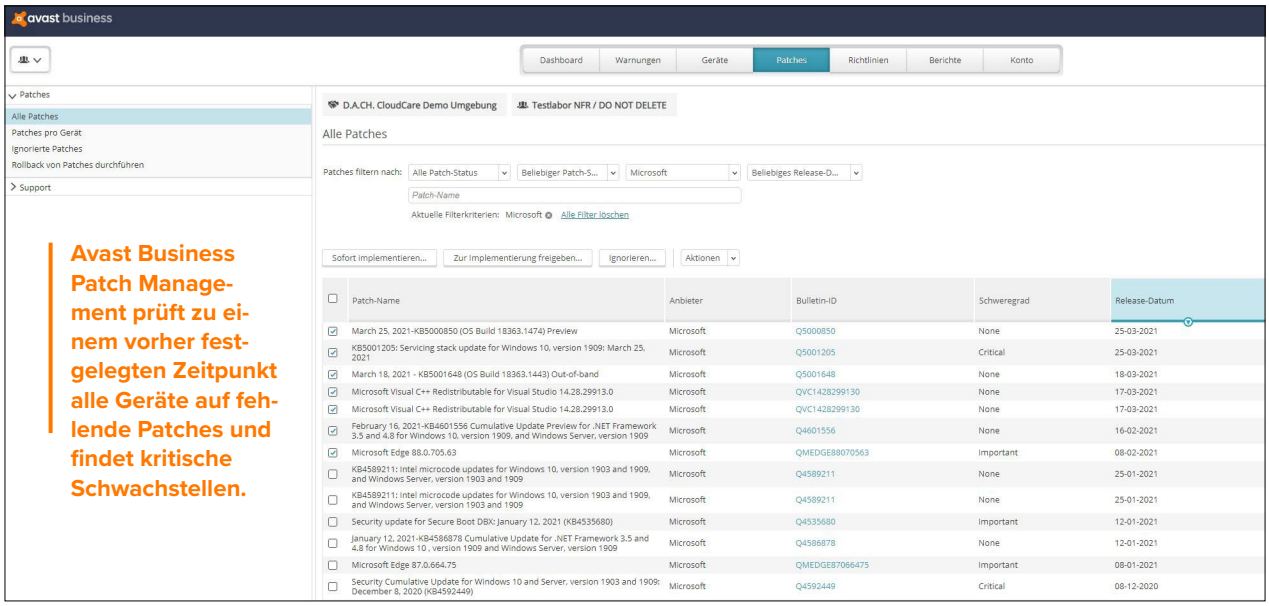
Ein solche Situation ist leider Alltag und betrifft jede Software in der IT-Infrastruktur. Das Sicherheitsunternehmen Avast stellte beispielsweise bei einer Sicherheitsmessung auf 500.000 Endgeräten fest, dass nur knapp ein Drittel die Patch-Tests bestanden haben. Lediglich 304 der Geräte waren vollständig aktualisiert.

Unternehmen können Patches zwar manuell einspielen. Aber das ist aufwendig – erst recht, wenn Mitarbeiter im Homeoffice arbeiten und Geräte außerhalb der firmeneigenen Infrastruktur aktualisiert werden müssen. Zudem wissen viele nicht, ob sie die Updates brauchen. Manche Firmen vernachlässigen das Patchen auch, weil es den Betriebsablauf stört oder weil sie fürchten, dass es Probleme bereitet.

Ein automatisches Patch Management schützt vor Sicherheitslücken

Diese Herausforderungen löst ein modernes Patch-Management-System wie das „Business Patch Management“ von Avast für Windows:

- Das Tool prüft zu einem vorher festgelegten Zeitpunkt alle Geräte auf fehlende Patches und findet kritische Schwachstellen.
- Jede Software von hunderten von Anbietern wird auf allen Geräten automatisch aktualisiert, vom Betriebssystem bis zu Programmen.



Avast Business Patch Management prüft zu einem vorher festgelegten Zeitpunkt alle Geräte auf fehlende Patches und findet kritische Schwachstellen.

- Das läuft unabhängig vom Standort ab, egal, ob sich die Geräte im Homeoffice oder hinter einer Firewall befinden.
- Die Patches sind bereits getestet.
- Über ein Dashboard können Unternehmen auf einen Blick sehen, welche Patches fehlen, gerade aufgespielt werden und wie gefährlich die Sicherheitslücke war.

Mit dem Business Patch Management gewinnen Unternehmen nicht nur Sicherheit, sondern sparen auch Zeit und Aufwand. Das entspricht **Schritt 5** („Schwachstellen identifizieren und vor Schad-Software schützen“), die aus dem IT-Grundschutz des BSI abgeleitet sind (siehe Seite 7).

Eine Firewall im Netzwerk

Das Einspielen von Sicherheits-Updates ist nur einer der Bausteine, mit denen Unternehmen für mehr IT-Security sorgen. Andere Schritte umfassen den Schutz der Netzwerke, Schnittstellen und aller Endgeräte, Firewall und Virenschutz sowie der sichere Zugriff auf Unternehmensressourcen. Hilfreich sind dafür Sicherheitslösungen, die auf die Bedürfnisse von KMUs ausgerichtet sind und die ihre Aufgaben automatisch erledigen. Die Lösung „Avast Business“ bietet einen mehrschichtigen Schutz, um Benutzer und IT-Ressourcen gegen Bedrohungen abzusichern.

Der Datenverkehr im Internet besteht heute zu fast 90 Prozent aus verschlüsseltem Datenverkehr. Ältere Firewall-Appliances sind nicht in der Lage, diesen auf Angreifer zu untersuchen. Wenn darüber beispielsweise Ransomware-Angriffe erfolgen, werden sie nicht erkannt.

Das „Secure Internet Gateway“ (SIG) von Avast kann dagegen den SSL-TLS-Datenverkehr umfassend und schnell überprüfen. Die Unified-Threat-Management-Lösung arbeitet in der Cloud und in Echtzeit. Sie wurde speziell für KMUs entwickelt und schützt alle Geräte der Firma vor Attacken aus dem Netz – unabhängig von Standort, Betriebssystem oder Netzwerk. Mitarbeiter im Homeoffice mit Android-Smartphone oder iPhone werden ebenfalls geschützt. Auch der sichere Zugriff auf Cloud-Applikationen wie Office 365 mit Microsoft Teams ist so gewährleistet.

Das entspricht **Schritt 4** („Unternehmensnetzwerke und Schnittstellen absichern“) und **Schritt 8** („Alle Endgeräte schützen“), die aus dem IT-Grundschutz des BSI abgeleitet sind (siehe Seite 7 und 8).

Sicherer Zugriff auf interne Anwendungen

Mitarbeiter sollen aus der Ferne auf Programme zugreifen können, die im Firmennetzwerk laufen? Möglich ist das mit einer Sicherheitslösung für den Remote-Zugriff. Ausschließlich autorisierte Nutzer können dann schnell Anwendungen aufrufen. Gängig sind hierfür oft VPN-Tools. Aber der cloudbasierte Avast „Secure Private Access“ (SPA) hat Vorteile gegenüber VPN: Der Zugang über die Zero-Trust-Network-Access-Lösung erfolgt nahtlos, unkompliziert und ohne zusätzlichen Client. Eine Hardware-Infrastruktur ist nicht notwendig. Außerdem gelangen Anwender nie ins Netzwerk selbst. Auch auf Cloud-Anwendungen und private Informationen kann so sicher zugegriffen werden.

Das entspricht **Schritt 3** („IT-Systeme sicher konfigurieren“) und **Schritt 8** („Alle Endgeräte schützen“), die aus dem IT-Grundschutz des BSI abgeleitet sind (siehe Seite 7 und 8).

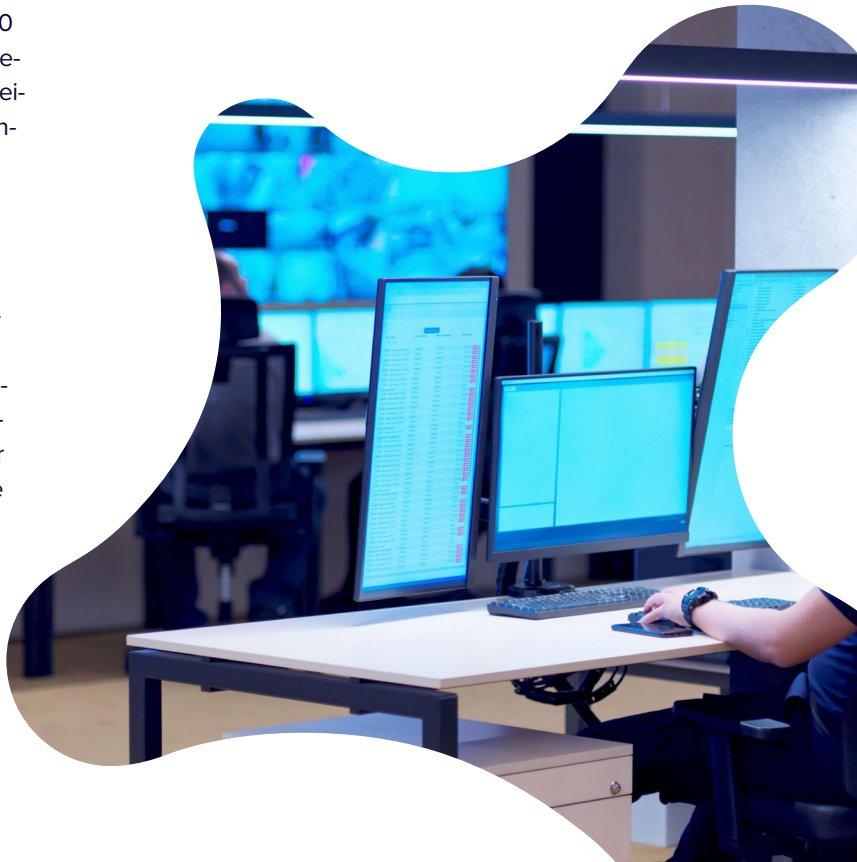


Bild: Shock / Bigstock

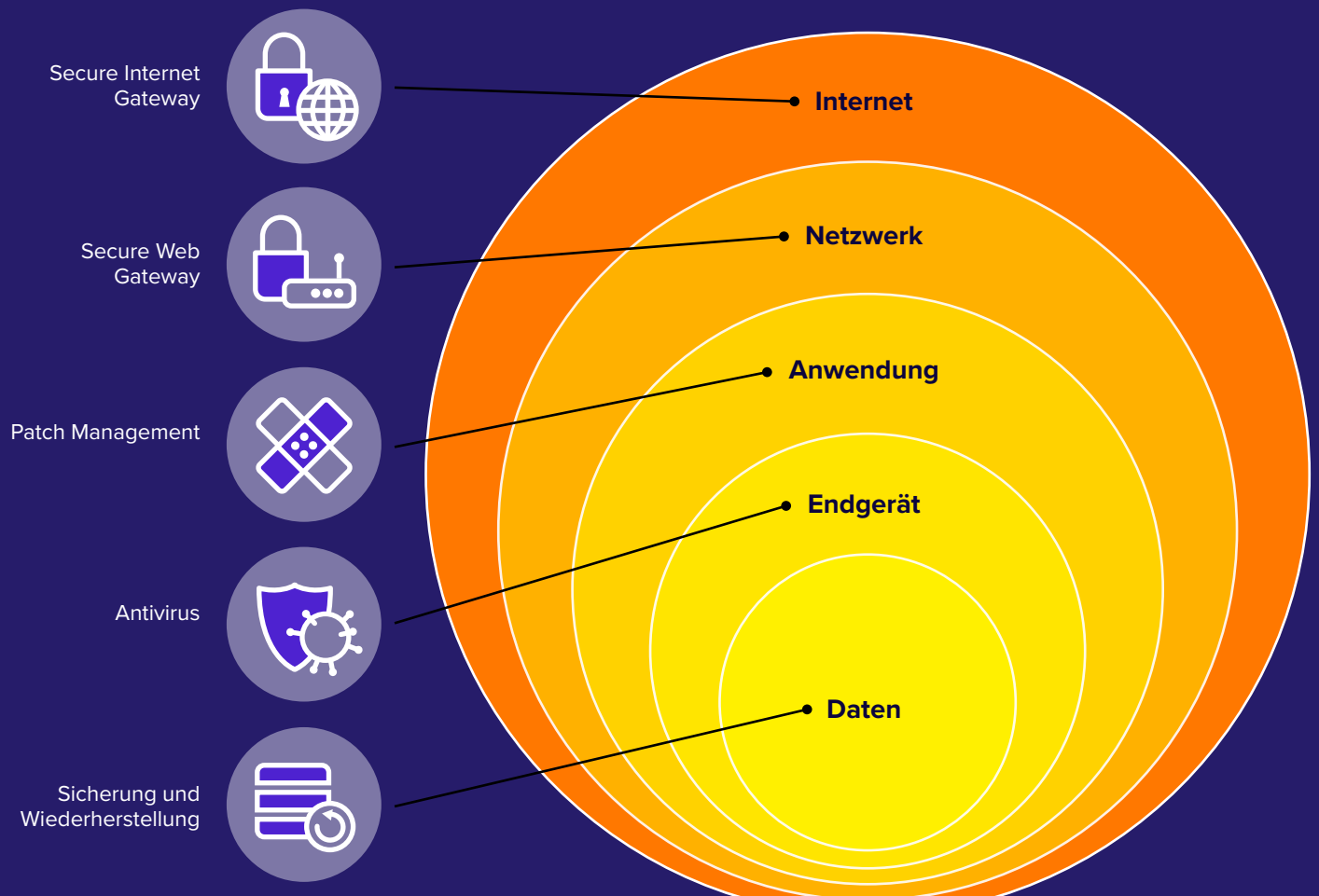
Schutz vor infizierten Webseiten

Die Sicherheit gefährden können jedoch die Beschäftigten selbst – beispielsweise, indem sie Webseiten mit Schad-Software aufrufen oder auf Phishing hereinfallen und dann infizierte Daten herunterladen. Den Zugriff sowohl auf Schad-Software-Seiten als auch auf Downloads sperrt der Avast „Business Secure Web Gateway-Dienst“. Damit werden Angreifer zugleich daran gehindert, auf diesem Weg in das Netzwerk einzudringen. Der Web- und Content-Filter ist cloudbasiert und schützt in Echtzeit sowohl einzelne Mitarbeiter mit Mobilgeräten als auch ganze Netzwerke vor Malware. Unternehmen können zudem Listen für erlaubte oder gesperrte Webseiten erstellen.

Das entspricht **Schritt 6** („E-Mails und Internet sicher nutzen“) und **Schritt 8** („Alle Endgeräte schützen“), die aus dem IT-Grundschutz des BSI abgeleitet sind (siehe Seite 7 und 8).

Mehrstufige Sicherheit – eine umfassende Lösung

Zusätzliche Sicherheitsstufen sind ein wichtiger Teil einer umfassenden Schutzstrategie.



Grafik: Eismann / stroemung GmbH

Den Überblick behalten

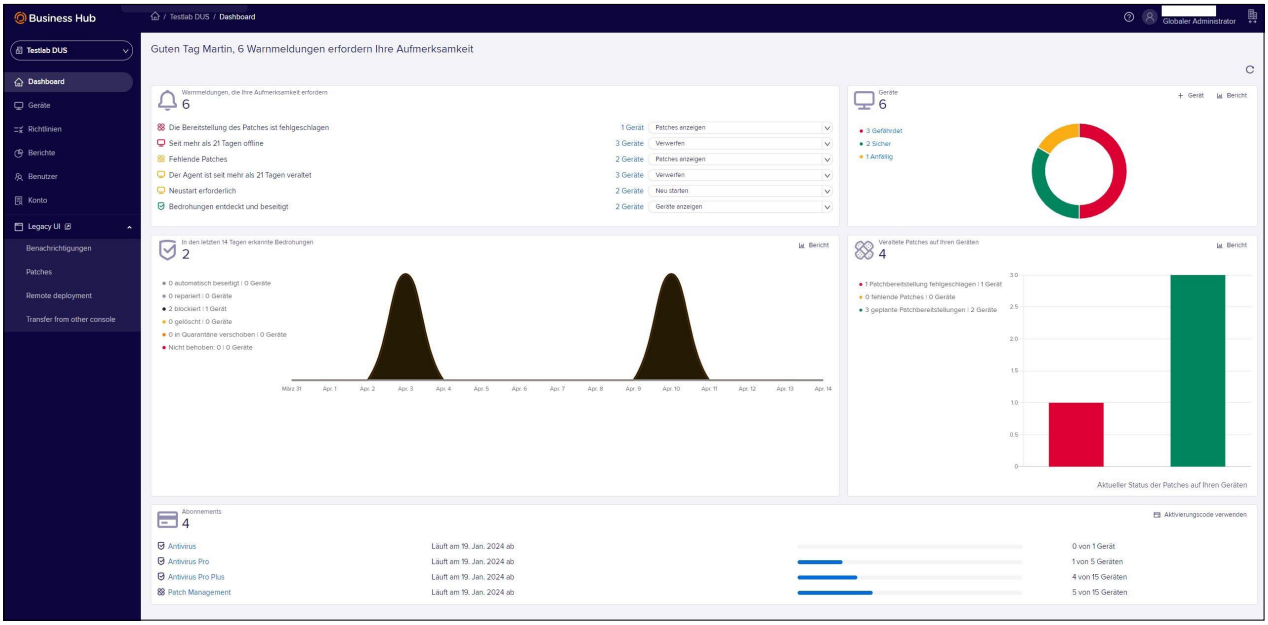
Die Programme bereitstellen und verwalten können Unternehmen über eine zentrale Plattform, das ebenfalls cloudbasierte Avast „Business Hub“. Es sendet umgehend einen Alarm, wenn es Sicherheitsprobleme gibt. Außerdem ermöglicht es eine Geräte- und Richtlinienverwaltung und verschafft mit Berichten Überblick über alle Aktivitäten.

Über die Konsole können auch andere Lösungen der Sicherheitsexperten integriert werden, etwa die Endpoint-Protection-Lösung „Business Antivirus“ für alle Geräte im Netzwerk. Sie spürt Viren, Würmer, Trojaner und andere Schad-Software auf. Außerdem lässt sich ein Backup- und Wiederherstellungs-Tool integrieren.

Das entspricht **Schritt 5** („Schwachstellen identifizieren und vor Schad-Software schützen“), **Schritt 8** („Alle Endgeräte schützen“) und **Schritt 9** („Daten sichern und für den Notfall vorsorgen“),die aus dem IT-Grundschutz des BSI abgeleitet sind (siehe Seite 7 und 8).

Die digitale Transformation ist für viele KMUs unvermeidlich geworden. Sie eröffnet viele Chancen, beispielsweise agileres Arbeiten, mehr Flexibilität sowie größere Effizienz. Gleichzeitig werden Firmen durch die Digitalisierung anfällig für immer neue und komplexe Bedrohungen. Mithilfe auf sie abgestimmter Sicherheitslösungen können sie Schwachstellen minimieren – und so dafür sorgen, dass die IT-Infrastruktur sicher und geschützt genutzt werden kann. Die Mitarbeiter können sich auf ihre Kernaufgaben konzentrieren, Prozesse werden verbessert, aber gleichzeitig die Budgets nicht überstrapaziert.

Avast Business Hub sendet umgehend einen Alarm, wenn es Sicherheitsprobleme gibt und verschafft mit Berichten Überblick über alle Aktivitäten.



avast business

DATENBLATT

Business Hub

Managed Security Plattform für Unternehmen

Der Business Hub ist eine leistungsstarke Cloud-basierte Plattform, mit der Unternehmen alle in ihren Netzwerken bereitgestellten Avast Business-Lösungen verwalten können. Es bietet Echtzeit-Transparenz zu Bedrohungen sowie umfassende Berichts- und Verwaltungsfunktionen auf einer einzigen Plattform.

Überwachen Sie Bedrohungen von einem einzigen Dashboard aus

Konfigurieren Sie auf Geräteaktionen basierende Benachrichtigungen und überwachen Sie diese über ein zentrales Dashboard, um vollständige Transparenz über einzelne Geräte und über mögliche Bedrohungen zwischen verknüpften Geräten zu erhalten.

Mandantenfähigkeit

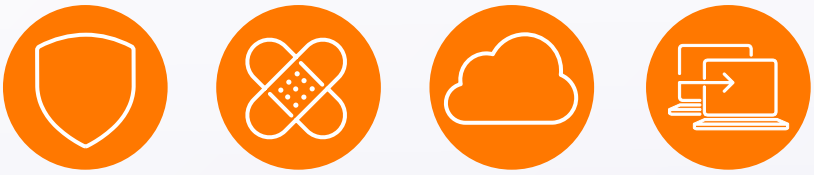
Verwalten Sie einfach mehrere Stätten oder Standorte und optimieren und vereinheitlichen Sie die Verantwortlichkeiten in großen Teams. Es können zum Beispiel mehrere Benutzer mit begrenztem Zugriff auf bestimmte Teile des Business Hub erstellt werden.

Sicherheit auf Enterprise-Level

Cloud-basierte Endpoint-Protection- und Netzwerksicherheitslösungen bieten umfassenden Schutz vor allen Formen von Malware und anderen Cyber-Bedrohungen - unabhängig davon, ob diese von innerhalb oder außerhalb des Netzwerks von E-Mail, über Websites oder über das Internet stammen.

Stellen Sie eine sichere Verbindung zu jedem verwalteten Gerät her

Verwenden Sie unser kostenloses Remote-IT-Tool, um eine sichere Verbindung zu jedem Gerät mit einem installierten Avast-Agenten herzustellen und um aus der Ferne Probleme zu beheben, Aufgaben auszuführen, Computer neu zu starten, Dateien zu übertragen und mit Benutzern zu chatten.



Funktionen

Intuitives Dashboard

Sie können alle Warnungen auf einen Blick sehen, Probleme beheben und Informationen erhalten, um fundierte Entscheidungen zu treffen, Dienste hinzuzufügen und schnell Maßnahmen zu ergreifen, um die Betriebszeit, Skalierbarkeit und Sicherheit zu erhöhen.

Geräte- und Richtlinienverwaltung

Verwalten Sie die Sicherheit für alle Geräte mit dem Business Hub-Agenten. Richtlinienänderungen werden automatisch in Echtzeit auf den vom Agenten gesteuerten Geräten konfiguriert, was weniger Wartung erfordert und die Skalierung des Geschäftsbetriebs erleichtert.

Detaillierte Berichte

Generieren und planen Sie einfach zu lesende, detaillierte Aktivitätsberichte mit einem Klick. Lassen Sie sich Berichte anzeigen, die blockierte Bedrohungen, Aufgabenlisten, geschützte Geräte, Patch-Status und mehr enthalten.

Benachrichtigungen

Erhalten Sie sofortige E-Mail-Benachrichtigungen zu Sicherheitsbedrohungen oder Netzwerkproblemen, einschließlich veralteter Antivirenanwendungen, erweiterter Geräteaktivität und zusätzlichen Geräte-Updates.

Master-Agent

Bestimmen Sie ein Gerät als lokalen Update-Server, auf den alle Updates heruntergeladen werden können. Sparen Sie Bandbreite, indem Sie Updates für alle Endgeräte in Ihrem Netzwerk planen und verteilen, wann immer es angebracht erscheint.

Befehle

Wenden Sie schnell Befehle wie Scans, Neustarts und mehr auf Geräten an und führen Sie auf Richtlinieneinstellungen basierende Befehle automatisch aus.

Dienste

Next-Gen Antivirus

Multi-OS AV verhindert, dass Cyberthreats in Ihr Netzwerk gelangen, schützt vor Zero-Day-Angriffen und identifiziert neue Bedrohungen.

Next-Gen Antivirus Pro

Erhalten Sie zusätzliche Sicherheit dank Funktionen wie Daten-Schredder und Schutz für Exchange- und SharePoint-Server.

Next-Gen Antivirus Pro Plus

Holen Sie sich das komplette Virenschutzpaket mit SecureLine VPN, Browser Cleanup und Webcam-Schutz.

Patch Management

Bleiben Sie Sicherheitslücken immer einen Schritt voraus, indem Sie kritische Patches identifizieren und einfach auf allen Endgeräten bereitstellen – von einem zentralen Dashboard aus.

Premium Remote Control (Coming Soon)

Stellen Sie von jedem Ort aus eine sichere Verbindung zu jedem Gerät her, um Probleme aus der Ferne zu beheben, Aufgaben auszuführen, neu zu starten, Dateien zu übertragen und mit Ihren Benutzern zu chatten.

Cloud Backup (in Kürze erhältlich!)

Secure Web Gateway (in Kürze erhältlich!)

Secure Internet Gateway (in Kürze erhältlich!)

Über Avast Businessss

Avast bietet All-in-One-Cyber Security-Lösungen für den modernen Arbeitsplatz von heute und bietet absolute Sicherheit. Avast bietet integrierte, 100% Cloud-basierte Endpoint- und Netzwerksicherheitslösungen für Unternehmen und ITDienstleister. Das Avast Business-Sicherheitsportfolio wird vom größten, weltweit am weitesten verbreiteten Netzwerk zur Erkennung von Bedrohungen unterstützt und macht es einfach und kostengünstig, komplexe Netzwerke zu sichern, zu verwalten und zu überwachen. Unsere einfach zu implementierenden Cloud-Sicherheitslösungen bieten maximalen Schutz, auf den sich Unternehmen verlassen können. Weitere Informationen zu unseren Cloud-basierten Cyber Security-Lösungen finden Sie unter **www.avast.com/business**.

avast business

DATENBLATT

Patchverwaltung

Identifizieren kritischer Schwachstellen und schnelle Bereitstellung von Updates auf allen Endgeräten

Die Patchverwaltung spielt eine entscheidende Rolle bei der Endgerätesicherheit, doch viele Unternehmen sind zögerlich mit Patches, weil zu viele davon verfügbar sind, die Bereitstellung oft den Betrieb unterbricht und sie Probleme mit anderen Systemen verursachen können. Avast Business Patchverwaltung bereitet dem Ratespiel beim Patching ein Ende, indem sie Schwachstellen aufdeckt, die sich durch Patch-Bereitstellung über ein zentrales Dashboard ohne großen Aufwand beseitigen lassen.

Zeit- und Kosteneinsparungen durch Patch-Automatisierung

Verteilen Sie in Minutenschnelle gründlich getestete Patches unter Tausenden von Geräten mit nur minimalen Auswirkungen auf Ihr Netzwerk.

Patchen von Drittanbieter-Anwendungen

Unterstützung von Patches für Microsoft Windows und Hunderten von namhaften Anbietern und Produkten wie iTunes®, Oracle®, Java, Adobe® Flash® und Reader.

Patchen per Fernzugriff

Patchen Sie standortunabhängig sämtliche Windows-Geräte – egal, ob diese auf eine Reise mitgenommen wurden oder sich hinter der Firewall, an dezentralen Standorten oder gar im Energiesparmodus befinden.

Zentrale Verwaltung

Verwalten Sie Software-Updates über eine zentrale Konsole.

Eindämmen und Schließen von Schwachstellen

Erzielen Sie Compliance, dämmen Sie Exploits ein, schließen Sie Schwachstellen und stellen Sie per Remote Software- und Windows-Updates bereit.

1. Geräte scannen **2. Patches bereitstellen** **3. Status überprüfen**

Funktionen

Flexible Bereitstellungspläne
Die Bereitstellung genehmigter Patches kann zu einem zuvor festgelegten Zeitpunkt automatisch oder aber manuell für bestimmte Gruppen und einzelne Geräte erfolgen.

Intuitives Dashboard
Sie können alle Software-Patches verwalten und erhalten für sämtliche verwalteten Geräte eine grafische Übersicht über alle installierten, fehlenden oder fehlgeschlagenen Patches.

Konfigurierbare Patches
Patch-Scans und -Installationen können nach Softwareanbieter, Produkt oder Patch-Schweregrad erfolgen. Erstellen Sie mühelos Ausnahmen für Anwendungen.

Master-Agent-Funktionen
Laden Sie alle fehlenden Patches auf einen Master-Agent herunter, der sie nahtlos auf alle verwalteten Geräte im Netzwerk verteilt.

Patch-Scan-Ergebnisse
Sehen Sie detaillierte Ergebnisse über eine zentrale Plattform ein, die Informationen zu fehlenden Patches, die jeweiligen Schweregrade, Wissensdatenbank-Links, Veröffentlichungsdaten, Beschreibungen und mehr enthält.

Umfassende Berichte
Ermitteln Sie einfach und schnell den Zustand und die Sicherheit von Gerätesoftware mittels einer Vielzahl leicht konfigurierbarer Berichte.

Automatische Scans
Legen Sie eine automatische Ausführung von Patch-Scans in 24-Stunden-Abständen oder aber eine automatische Bereitstellung von Patches an jedem Donnerstag fest. Diese Standardeinstellungen lassen sich beliebig anpassen.

Tausende Patches
Für umfassenden Schutz werden Patches für Windows-Betriebssysteme und Tausende weiterer Softwareanwendungen von Drittanbietern bereitgestellt.

Patch-Rollbacks
Deinstallieren Sie einfach Patches von einzelnen Geräten, wenn sich diese als instabil erweisen oder Probleme auftreten, damit Ihre Benutzer ohne Downtimes weiterarbeiten können.

Patch-Freigaben
Dies ist ein Sicherheitsmechanismus, dank dem Sie die Übersicht darüber behalten, welche Patches zur Bereitstellung freigegeben wurden und welche nicht.

Über Avast Business

Avast bietet All-in-One-Cyber Security-Lösungen für den modernen Arbeitsplatz von heute und bietet absolute Sicherheit. Avast bietet integrierte, 100% Cloud-basierte Endpoint- und Netzwerksicherheitslösungen für Unternehmen und IT-Dienstleister. Das Avast Business-Sicherheitsportfolio wird vom größten, weltweit am weitesten verbreiteten Netzwerk zur Erkennung von Bedrohungen unterstützt und macht es einfach und kostengünstig, komplexe Netzwerke zu sichern, zu verwalten und zu überwachen. Unsere einfach zu implementierenden Cloud-Sicherheitslösungen bieten maximalen Schutz, auf den sich Unternehmen verlassen können. Weitere Informationen zu unseren Cloud-basierten Cyber Security-Lösungen finden Sie unter **www.avast.com/business**.

avast business

DATENBLATT

Secure Internet Gateway

Avast Business Secure Internet Gateway (SIG) ist eine revolutionäre Cloud-basierte Unified-Threat-Management-Lösung, die lokale Appliances überflüssig macht. SIG bietet einen unternehmenstauglichen Schutz für kleine und mittlere Unternehmen vor den immer raffinierter werdenden Cyberkriminellen von heute. Dank seiner fortschrittlichen Sicherheitstechnologien bietet Secure Internet Gateway einen zuverlässigen Echtzeitschutz gegen Web- und Internet-Bedrohungen für alle Geräte, Standorte und Nutzer.

Erweiterte Sicherheit

Das Secure Internet Gateway (SIG) von Avast Business bietet einen umfassenden Security Stack mit allen tiefgreifenden Sicherheitsmechanismen, die Sie jemals benötigen werden. SIG wird über die weltweit größte Sicherheits-Cloud als Dienstleistung angeboten und bietet eine tiefgründige Paketprüfung über alle Ports und Protokolle hinweg – dies umfasst auch mit SSL verschlüsselten Datenverkehr.

Geringere Gesamtbetriebskosten

Befreien Sie sich mit unserer kompletten Cloud-basierten Lösung von teuren Hardware-Sicherheitseinrichtungen, Hardware-Wartungsplänen, komplizierter Verwaltung und Kosten für die Umleitung von Datenströmen aus verteilten Standorten. Sie brauchen keine Hardware zu kaufen, bereitzustellen und zu verwalten.

Schützen Sie alle Benutzer

Dank unserer Cloud-basierten Lösung können Sie sich von teuren Hardware-Sicherheits-Appliances, Wartungs-Upgrades für Hardware, einer komplizierten Verwaltung und Kosten für den Backhaul-Datenverkehr von und zu dezentralen Niederlassungen verabschieden. SIG ist kompatibel mit Ihrem bestehenden Netzwerk, sodass Sie keine zusätzliche Hardware erwerben, bereitstellen oder verwalten müssen.

Schützen Sie alle Benutzer

Mit der Cloud-basierten Internet-Sicherheitslösung mit Echtzeitschutz, die Daten aus über 60 Feeds mit Informationen zu Bedrohungen abruft, über 65 Milliarden Transaktionen pro Tag verarbeitet und täglich 125.000 Updates an bis dato über 150 Rechenzentren sendet, können

“Zusätzlich zu der stark verbesserten Sicherheit kann die Lösung einfach und schnell bereitgestellt werden, ohne dass das laufende Geschäft beeinträchtigt wird. Das Secure Internet Gateway verbessert die Arbeitsabläufe des MSSP. “

CHAD STRADER, PRÄSIDENT VON KAPPA SERVICES.

“Mit Secure Internet Gateway-Diensten hat Boca West seine hochmoderne Sicherheit weiter ausgebaut und ist nun bereit, es mit allen zukünftigen Herausforderungen aufzunehmen.”

NORMAN LANDERMAN, SDSI.

“Das Avast Secure Internet Gateway ist die perfekte Mischung aus einem globalen Sicherheitsnetzwerk und einem Cloud-verwalteten Firewall-Dienst, die zusammenarbeiten, um die Sicherheitsanforderungen von Geschäftskunden an mehreren Standorten zu erfüllen”,

JULIAN JACQUEZ, PRÄSIDENT UND COO VON BCN.

Sie all Ihren Benutzern einen umfassenden Schutz bieten, egal wo diese sich gerade befinden. Schützen Sie Ihre Belegschaft von dezentralen und mobilen Mitarbeitern, indem Sie einfach eine App installieren, die mit allen Betriebssystemen kompatibel ist.

Unendliche Wachstumsmöglichkeiten

Richten Sie in nur wenigen Stunden neue Standorte über ein zentrales Dashboard ein. Bei einer Expansion in neue Bürostandorte, erstellen Sie einfach einen neuen Standort und ordnen Sie ihm die entsprechenden Regeln zu. Und schon sind Sie startklar! Im Gegensatz zu herkömmlichen Security Appliances wird Avast SIG automatisch an die Bandbreite und die Kapazitätsanforderungen angepasst.

Optimierte Verwaltung

Überwachen Sie mehrere Standorte und Roaming-Nutzer von einer einheitlichen Cloud-Konsole aus. Flexible Richtlinien helfen bei der Bereitstellung von Sicherheitsdiensten, der Verwaltung von Firewall-Regeln, der Bereitstellung von Echtzeit-Transparenz und einer Drilldown-Übersicht für jeden Benutzer, um Ereignisse zu korrelieren und Bedrohungen zu beseitigen.

Cloud-basierte Sicherheitsplattform

Secure Internet Gateway wird von einer Sicherheitsarchitektur der nächsten Generation getragen, die ganz auf Leistung und Skalierbarkeit ausgelegt ist. Es ist auf über 150 Rechenzentren auf 6 Kontinenten verteilt und bietet somit hohe Geschwindigkeiten und eine stets ausreichende Kapazität.

	SIG	SIG Advanced	SIG Total
Cloud-basierte Sicherheitsplattform			
Rechenzentren Weltweiter Zugriff und hohe Verfügbarkeit mit durch SLAs zugesicherter Latenz. .	●	●	●
Automatische Echtzeit-Updates Über 125.000 tägliche Updates aus über 60 Feeds mit Informationen zu Bedrohungen.	●	●	●
Granulare Richtlinien, die bei den Benutzern überall auf der Welt forciert werden.	●	●	●
Authentifizierung SAML, Secure LDAP, Kerberos, gehostet.	●	●	●
Client-App zur Absicherung mobiler Geräte (Windows, Mac, Android)	●	●	●
Traffic Forwarding GRE-Tunnel, IPSEC, PAC, Proxy Chaining oder Client Connector	●	●	●
Service Level Agreement (SLA) für hohe Verfügbarkeit und niedrige Latenzen	●	●	●
SSL-Prüfung			
Umfassende Inline-Bedrohungsprüfung des gesamten SSL-/TTS-Datenverkehrs inklusive SLA und granularer Richtlinie	●	●	●

avast business

	SIG	SIG Advanced	SIG Total
URL und Content Filtering			
Filtern nach Richtlinien über 6 Klassen, 30 übergeordnete Kategorien und 90 Kategorien hinweg	●	●	●
Dynamische Klassifizierung von Inhalten für unbekannte URLs und Safe Search	●	●	●
Granulare Richtlinien nach Benutzer, Gruppen, Standorten, Zeiten und Quoten	●	●	●
Inline-Antivirus und -Anti-Spyware			
Signaturbasierter Anti-Malware-Schutz und vollständige Prüfung von ein- und ausgehenden Dateien.	●	●	●

	SIG	SIG Advanced	SIG Total
Übersicht und Kontrolle über Cloud-Anwendungen			
Entdecken und überwachen Sie Web-Anwendungen (Streaming, soziale Medien, E-Mails usw.)	●	●	●
Granulare Steuerelemente für Webanwendungen	○	●	●
Cloud Identity Broker	○	●	●
Berichte und Kontrolle über mobile Anwendungen			
Granulare Richtlinien und Berichte über mobile Anwendungen und Geräte	●	●	●
Cloud Firewall			
Standard-Cloud-Firewall Regeln nach Standorten, IP-Adressen, Ports und Protokollen	●	●	●
Erweiterte Cloud-Firewall Umfassende Layer-7-Cloud-Firewall für ausgehenden Datenverkehr und IPS	○	○	●
Umfassende Firewall-Protokollierung Detaillierte Protokolle, statistische Berichte und Dashboards	○	○	●
Webzugriffssteuerung			
Stellen Sie sicher, dass veraltete und anfällige Browser und Plugins den Anforderungen entsprechen	○	●	●

	SIG	SIG Advanced	SIG Total
Kontrolle über die Bandbreite			
Schützen Sie essentielle Apps und schränken Sie Freizeitanwendungen standort- und tageszeitabhängig ein	○	●	●
Erweiterter Schutz vor Bedrohungen			
Echtzeit-Feeds zum rufbasierten Sperren von Phishing-Seiten und Botnets	●	●	●
Blockieren von Malware, Spyware und bösartigen Webseiten	○	●	●
Cloud-basiertes IPS zum Blockieren von Signaturen komplexer Bedrohungen für HTTP und HTTPS	○	●	●
Blockieren von Cross Site Scripting (XSS), Cookie-Diebstahl bösartiger aktiver Inhalte.	○	●	●
Cloud Sandbox			
Standardmäßige Cloud-basierte Sandbox: Schutz vor Zero-Day-Angriffen über .exe- und .dll-Dateien von unbekannten oder verdächtigen Webseiten	●	●	●
Erweiterte Cloud-basierte Sandbox: Schutz vor Zero-Day-Angriffen über jeden Dateityp, Quarantäne je nach Richtlinie, detaillierte Berichte	○	○	●
Echtzeitberichte und -protokolle			
6 Monate, globale gegenseitig bedingte interaktive Echtzeit-Berichte	●	●	●
Streamen an das Vor-Ort-SIEM (Nanolog Streaming Service mit Live-Management)	○	●	●
Data Loss Prevention			
True File Type Control – Steuerung nach Benutzern, Gruppen und Zielen	●	●	●
Erweiterte Inline-DLP-Scans zum Verhindern von Datenaustritt aus dem Unternehmen	Add-on	Add-on	Add-on

Über Avast Business

Avast bietet All-in-One-Cyber Security-Lösungen für den modernen Arbeitsplatz von heute und bietet absolute Sicherheit. Avast bietet integrierte, 100% Cloud-basierte Endpoint- und Netzwerksicherheitslösungen für Unternehmen und IT-Dienstleister. Das Avast Business-Sicherheitsportfolio wird vom größten, weltweit am weitesten verbreiteten Netzwerk zur Erkennung von Bedrohungen unterstützt und macht es einfach und kostengünstig, komplexe Netzwerke zu sichern, zu verwalten und zu überwachen. Unsere einfach zu implementierenden Cloud-Sicherheitslösungen bieten maximalen Schutz, auf den sich Unternehmen verlassen können. Weitere Informationen zu unseren Cloud-basierten Cyber Security-Lösungen finden Sie unter **www.avast.com/business**.