Bitdefender®

IT-SICHERHEIT IM DIGITALISIERTEN GESUNDHEITSWESEN

Sicherheitsprozesse automatisieren
Schutzschichten konsolidieren
IT-Security mit knappen Mitteln optimieren

Bitdefender

MANAGEMENT SUMMARY

Der Healthcare-Sektor hat ganz eigene IT-Sicherheitsherausforderungen, etwa hinsichtlich der elektronischen Patientenakte (ePA) oder vernetzten Medizingeräten.

Die Digitalisierung ist zugleich unumgänglich, um im Gesundheitswesen mit Gewinn zu wirtschaften. Sie kann nur gelingen, wenn alle beteiligten Einrichtungen und Unternehmen höchste Sicherheitsstandards aufbauen.

Ziel ist es insbesondere, sich gegen Erpressung und Patienten vor Datendiebstahl zu schützen. Dies leistet ein vielschichtiger Schutz, der den Aufwand für die Angreifer potenziert und ihren möglichen finanziellen Nutzen minimiert.

Zu den wesentlichen Bestandteilen eines solchen Schutzes gehören Next Generation Anti-Malware, Enterprise Detection & Response (EDR), Schutz virtueller Systeme und eine Analyse des Datenverkehrs im Netzwerk.

Mithilfe von konsolidierten Lösungen, Machine Learning und Automatisierung können Healthcare-Unternehmen trotz des hohen Kostendrucks und des Mangels an IT-Personal diese Anforderungen meistern.

Bitdefender

INHALT

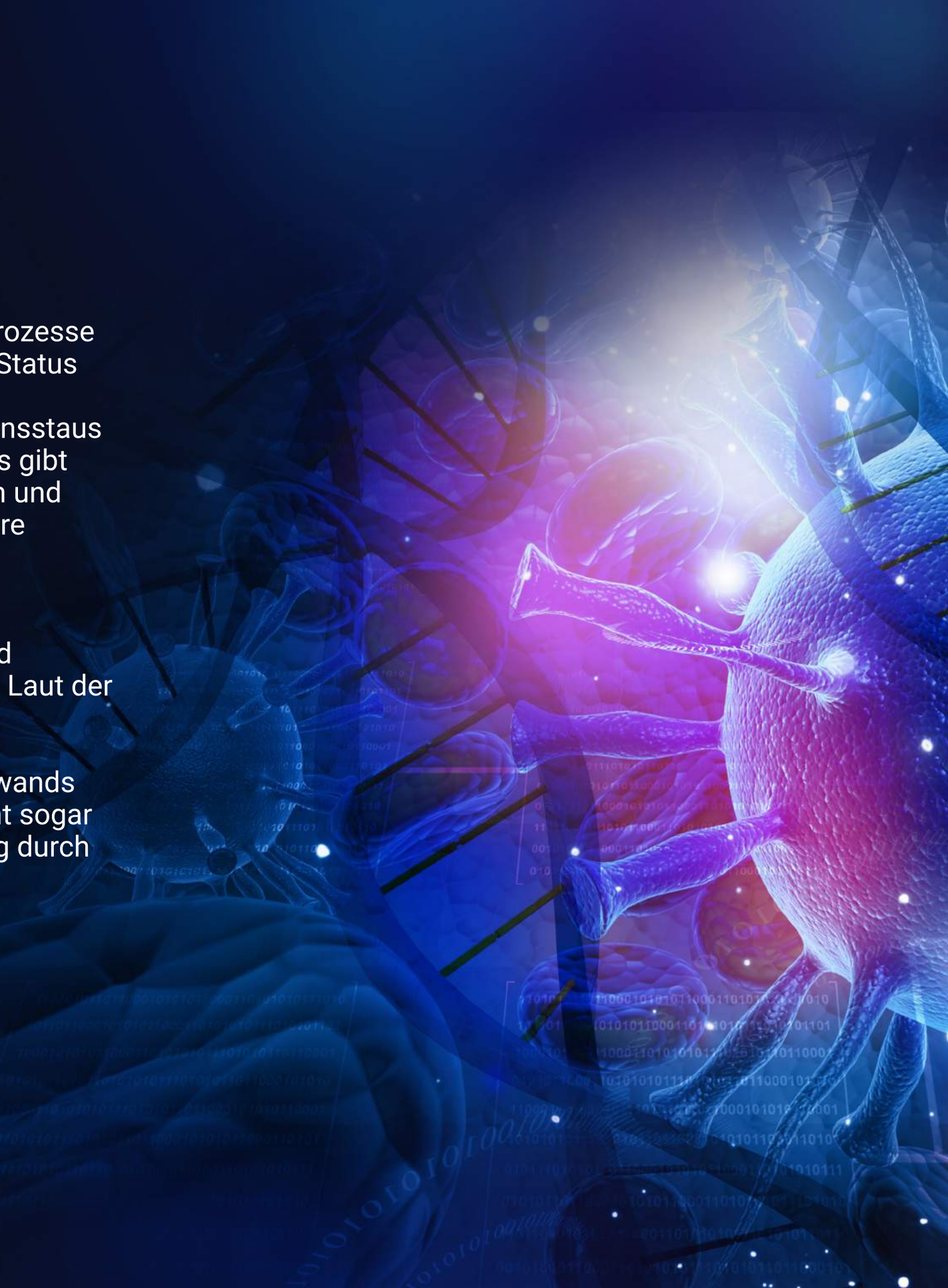
Bitdefender

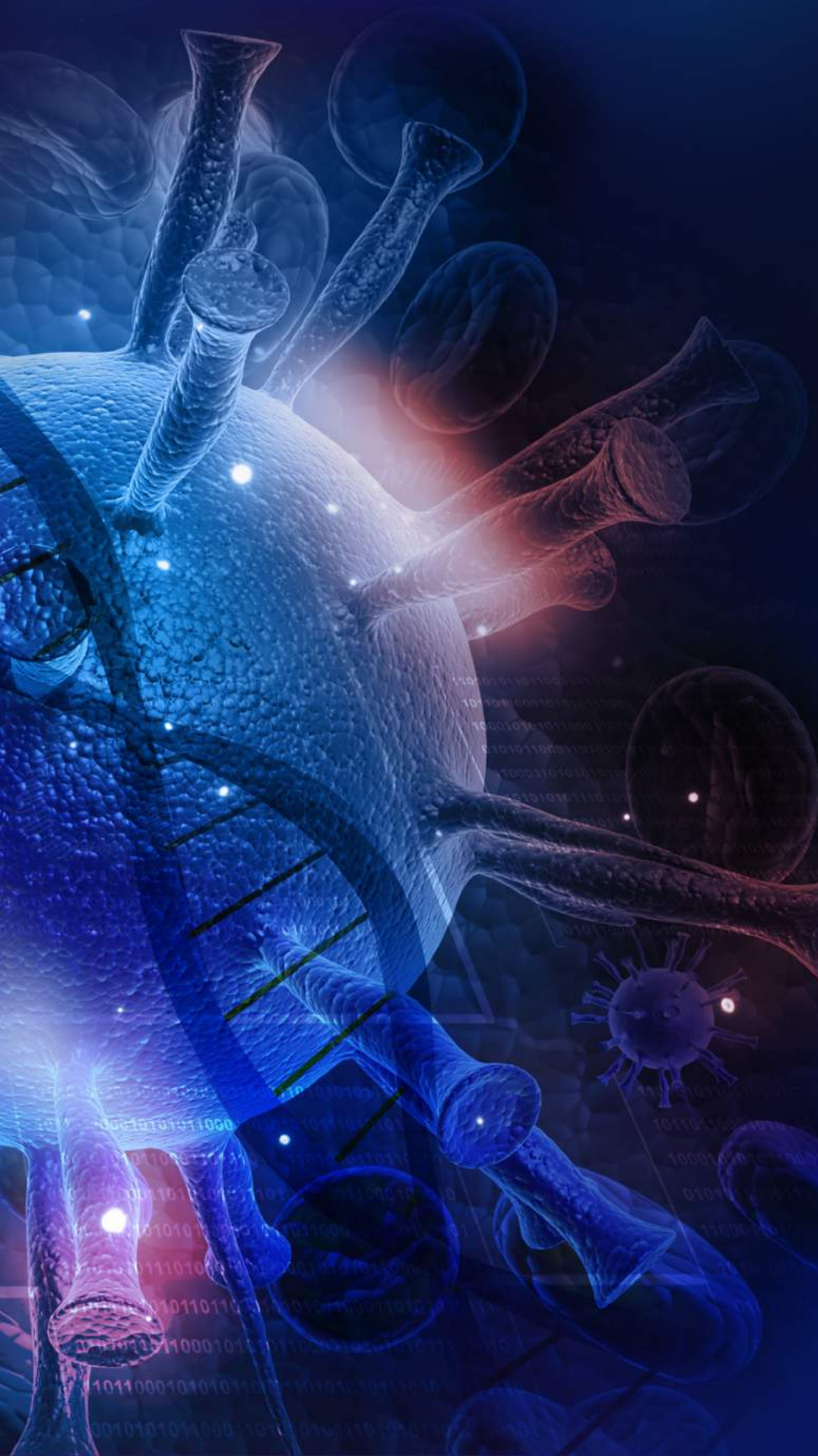
HEALTHCARE: FORTSCHRITT BRAUCHT VERTRAUEN

Bitdefender

Sicher ist sicher. Nach diesem Motto bleiben viele Prozesse im Healthcare-Sektor papierbasiert und analog. Der Status der IT-Ausstattung in vielen Krankenhäusern und Gesundheitseinrichtungen ist wegen eines Innovationsstaus und weiteren Gründen heute unbefriedigend. Doch es gibt kein Zurück: Das Gesundheitswesen digitalisiert sich und wird diesen Weg der technischen Innovation auf Jahre hinaus weiter gehen.

Klar ist: Nur über digitalisierte Prozesse werden Gesundheits-Einrichtungen auf Dauer kostendeckend arbeiten können und Gewinn erwirtschaften können. Laut der Unternehmensberatung McKinsey hätten sich durch Digitalisierung im Jahr 2018 im deutschen Gesundheitswesen rund 12 Prozent des Gesamtaufwands einsparen lassen. [1] Die Beratungsfirma PwC spricht sogar von 15 bis 20 Prozent potenzielle Effizienzsteigerung durch digitale Lösungen. [2]





Marktbeobachter gehen davon aus, dass die „Digitalisierung des Systems […] die Leistungen billiger machen und die Qualität verbessern“ kann.

[1] Gleichzeitig hat der Healthcare-Sektor im Zuge der Digitalisierung sehr viel höhere Hürden zu nehmen, als es etwa in der Industrie oder im Handel der Fall ist: eine ganz besondere Bedeutung von Vertrauen und eine existenzielle Sensibilität der Daten.

Es bedeutet eine hohe Anstrengung, intime Daten in einem Umfeld zu schützen, in dem es zugleich hilfreich und lebensrettend sein kann, dass legitime Anwender ganz verschiedener Organisationen auf die richtigen Daten Zugriff bekommen.

Dies zeigt sich am deutlichsten an der verzögerten Einführung der elektronischen Patientenakte (ePA).

Ganz besonders gefordert hinsichtlich IT-Security sind derzeit rund einhundert deutsche Krankenhäuser.

Bitdefender

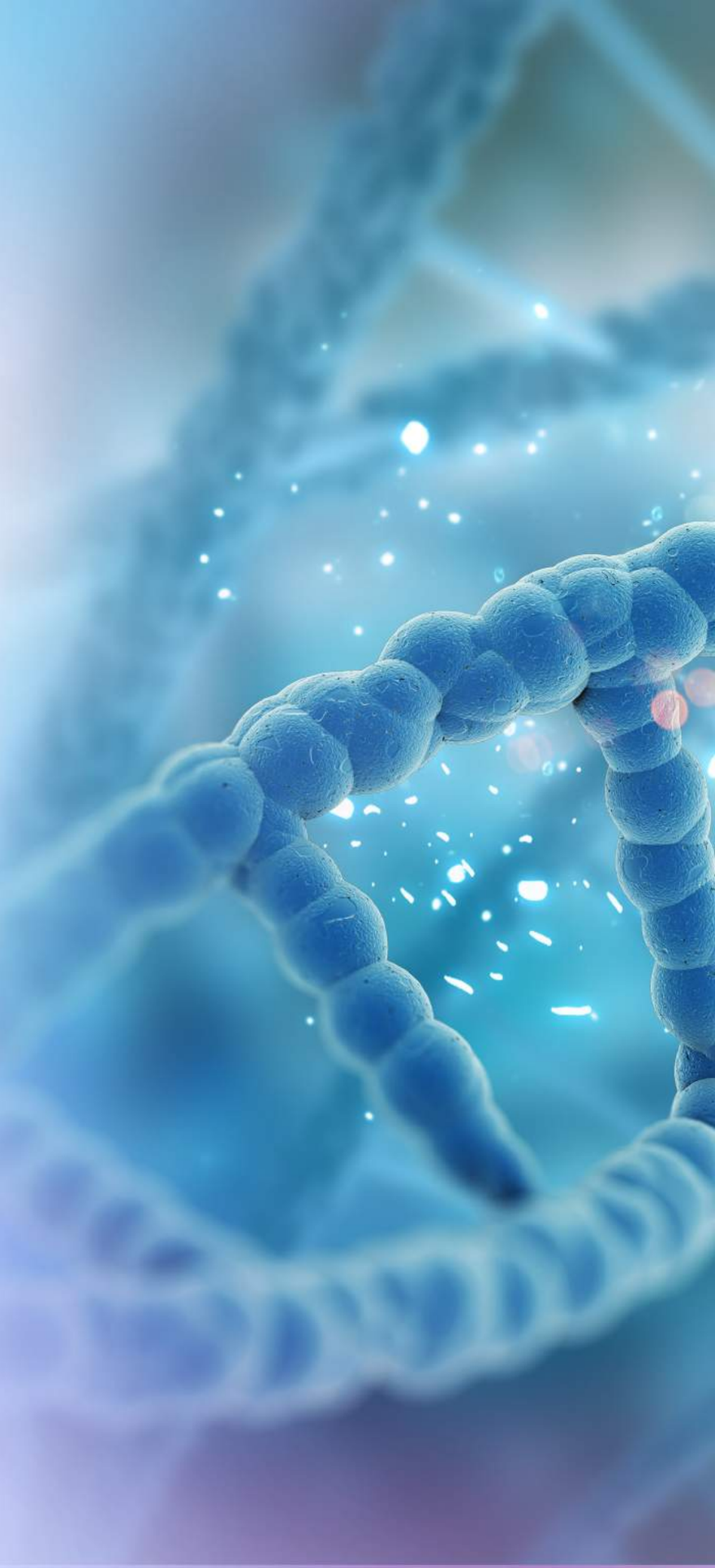
BESONDERE GEFAHREN ERFORDERN BESONDEREN SCHUTZ

Denn die größten Krankenhäuser Deutschlands müssen ab dem 1.

Juli 2019 als Teil der „kritischen Infrastruktur“ (KRITIS) ihre Resilienz unter Beweis stellen. Weil im Gesundheitssystem viele hochspezialisierte Einrichtungen miteinander arbeiten und auch Daten miteinander austauschen, stehen jedoch letztlich alle Einrichtungen und Firmen vor einer ähnlichen Herausforderung.

Auch Gesundheitszentren, Pharma-Unternehmen, Pflegeeinrichtungen, Apotheken, Arztpraxen, Träger-Organisationen, Krankenkassen, Labore, Hersteller medizinischer Geräte und Dienstleister, IT-Dienstleister und Leasinggeber haben die Aufgabe, sichere Strukturen für ein digital unterstütztes Gesundheitswesen mit seinen rund fünf Millionen Beschäftigten [3] zu schaffen.

Dies ist unter anderem deshalb eine Herkulesaufgabe, weil IT-Sicherheitsbeauftragte (ISB), IT-Leiter, IT-Manager, Security-Manager in der Branche ein Lied davon singen können, dass ihre Abteilungen chronisch unterbesetzt sind.



Die Gegner sind dagegen zahlreich und obendrein durch finanzielle Anreize hochmotiviert. Gesundheitsdaten sind bei kriminellen Organisationen begehrt. Und unzureichend geschützte Gesundheitseinrichtungen erscheinen Hackern als leichte Erpressungsopfer. Laut einer Studie der Unternehmensberatung Roland Berger wurden „64% der deutschen Krankenhäuser [...] schon einmal Opfer eines Hackerangriffs“. [4]

Bei der Digitalisierung in der Gesundheitsbranche sind Datensicherheit und Datenschutz somit unumstößliche Gebote. Dieses E-Book will den beteiligten IT-Fachleuten im Healthcare-Sektor, einschließlich Dienstleistern, Leasinggebern und sowie Produktmanagern und Prozessverantwortlichen bei Herstellern von Medizinprodukten einen Überblick über die aktuellen Herausforderungen, Bedrohungen und Lösungsansätze geben.

IT-Security ist der entscheidende Enabler, der Digitalisierung möglich macht und den Fortschritt beschleunigt. Die gute Nachricht ist, dass dies dank neuer Technologien auch mit maßvollen Mitteln und Personalressourcen möglich ist.

Bitdefender

DIE BESONDEREN IT-SICHERHEITSHERAUSFORDERUNGEN IM GESUNDHEITSWESEN

Bitdefender

Gesundheit ist ein höheres Gut als alle anderen. Die Digitalisierung der Gesundheitsbranche ist nicht nach dem Muster von Industrie, Logistik oder Handel zu haben. Sieben sicherheitsrelevanten Besonderheiten im Healthcare-Sektor sind diese:

1. **Elektronische Patientenakte (ePA)**
2. **Knappheit von IT-Fachpersonal**
3. **Sensibilität der Daten**
4. **Compliance-Anforderungen**
5. **Internet of Medical Things (IoMT)**
6. **Virtualisierungsgrad**
7. **Kostendruck**

1. ELEKTRONISCHE PATIENTENAKTE (EPA)

Die analoge, traditionelle Patientenakte wird allmählich zu Gunsten der patientenzentrierten, digitalen Gesundheitsakte am „Point of Care“ abgelöst. Der elektronischen Patientenakte (ePA) kommt eine Schlüsselstellung innerhalb der Digitalisierung der Branche zu.

Die McKinsey-Studie zur Digitalisierung im Gesundheitswesen untersucht das Einsparpotenzial von 26 Technologien und beziffert die Summe der möglichen Einsparungen auf 34 Milliarden Euro.

Die einheitliche elektronische Patientenakte macht davon annähernd ein Fünftel aus (6,4 Milliarden Euro), sonstige papierlose Daten weitere 2,6 Milliarden Euro. [1]

Es ist schwierig, eine ePA zu schaffen, die erstens dem Patienten die Hoheit über seine Daten lässt, zweitens sicher vor illegitimen Zugriff ist und drittens von allen berechtigen Parteien genutzt werden kann.

Dies zeigen verschiedenste privatwirtschaftliche Produkte und Apps, die allesamt dieses Ziel verfehlen.

Dennoch wird die ePA kommen. Sie ist seit dem Jahr 2004 gesetzlich verankert und laut Koalitionsvertrag der Bundesregierung von 2018 soll sie bis 2021 für jedermann verfügbar sein.

Klar ist, dass sie nur über eine Cloud-Infrastruktur implementiert werden kann. Es gibt die wirtschaftliche Notwendigkeit und einen klaren parteiübergreifenden politischen Willen für die ePA: „Für die erfolgreiche Weiterentwicklung unserer Gesundheitsversorgung ist das Vorantreiben der Digitalisierung die zentrale Voraussetzung.“ [3]

2. KNAPPHEIT VON IT-FACHPERSONAL

Im Vergleich zu Industrieunternehmen gleicher Größe sind Einrichtungen des Gesundheitswesens spärlich mit IT-Fachpersonal besetzt.

Angesichts der Herausforderungen könnte man vermuten, dass größere Einrichtungen normalerweise ein mehrköpfiges Team von IT-Experten vorhalten, mit dem sie auf Sicherheitsvorfälle reagieren können.

Doch dies ist aufgrund der damit verbundenen Kosten und dem allgemeinen Mangel an IT-Personal und IT-Sicherheitspersonal auf dem Arbeitsmarkt sehr selten.

Ein typischeres Setup ist zum Beispiel ein Team von nur drei Administratoren, das für die gesamte IT inklusive der IT-Sicherheit für einen Träger mit drei Krankenhäusern und über 1.500 klassischen Endpoints zuständig ist.

Große, privatwirtschaftlich organisierte Krankenhausketten mit zentralisierter IT sind in der Regel etwas besser ausgestattet.

Doch auch sie können beim „War for Talents“ nicht unbedingt mit Löhnen und Arbeitsbedingungen in anderen Branchen mithalten, welche die gleiche Expertise benötigen und stetige Gewinne reinvestieren können.

3. SENSIBILITÄT DER DATEN

Konstruktionspläne, technische Innovationen und Finanzdaten sind hoch sensible Daten.

Sie werden von Hackern bevorzugt gestohlen und von produzierenden Unternehmen oder Finanzdienstleistern sorgsam geschützt. Doch Gesundheitsdaten wie Diagnosen, Verordnungen und Röntgenbilder sind für den einzelnen Patienten oft noch viel sensibler.

Einerseits kann es lebenswichtig sein, dass bestimmte Daten, etwa zu Impfungen oder Vorerkrankungen im entscheidenden Moment verfügbar und abrufbar sind. Andererseits kann es das Leben eines Betroffenen schwer beeinträchtigen, wenn die Daten in die falschen Hände oder in die Öffentlichkeit geraten.

Wenn etwa eine HIV-Erkrankung oder eine Erbkrankheit bekannt werden, kann dies berufliche Karrieren gefährden, Menschen um ihren Versicherungsschutz bringen und noch negative Auswirkungen auf deren Kinder haben. Ohne Vertrauen ist die Arzt-Patientenbeziehung undenkbar. Deshalb ist Papier so lange ein beliebtes Medium und Fax ein beliebter Übertragungsweg geblieben.

Auch wenn man an Trends wie Personalisierte Medizin und Präzisionsmedizin denkt, die auf der Aggregierung von Gesundheitsdaten vieler Patienten basieren, muss die Medizin Wege finden, die Rückverfolgung der Daten unmöglich zu machen und vertrauenswürdig mit Daten umzugehen.

Denn bereits heute werden gestohlene Patientendaten im Darknet verkauft, es sind lukrative Informationen für Hacker.

4. COMPLIANCE-ANFORDERUNGEN

Das Gesundheitswesen ist hoch reguliert. Hier gilt nicht nur die DSGVO, die unter anderem verlangt, dass personenbezogene Daten nach dem Stand der Technik gesichert werden.

Für Medizingeräte gelten besondere Zertifizierungsvorgaben, darüber hinaus gibt es Patientenrechte, Entgeltgesetze, und Dutzende anderer Vorschriften, die alle eingehalten werden müssen.

Eine Sonderrolle nimmt das IT-Sicherheitsgesetz (IT-SiG) ein, das seit Juli 2015 in Kraft ist. Es definiert technische und organisatorische Anforderungen an kritische Infrastrukturen (KRITIS), u.a. Krankenhäuser mit mehr als 30.000 stationären Behandlungen jährlich. Dies betrifft etwa 100 der insgesamt rund 2.000 Krankenhäuser und einige weitere Einrichtungen in Deutschland.

Ab Juli 2019 müssen sich diese Einrichtungen einem Audit oder Zertifizierungen unterziehen.

Bußgelder können bis 100.000 Euro betragen.

Eine der Schwierigkeiten dabei: Welche Standards die IT im Detail einzuhalten hat, soll im Rahmen eines Branchenspezifischer Sicherheitsstandard „B3S“ definiert werden.

Dieser ist aber kurz vor dem Stichtag noch nicht fertiggestellt.

5. INTERNET OF MEDICAL THINGS (IOMT)

Eine neuere Entwicklung ist das Internet of Medical Things (IoMT), also der Trend, dass Medizingeräte vernetzt werden und somit Medizintechnik und IT verschmelzen. Das Beratungsunternehmen Frost & Sullivan schätzt, dass sich die Zahl der IoMT-Geräte bis 2020 von 4,5 Milliarden auf 20-30 Milliarden vervielfachen wird. [5]

Auch in anderen Branchen machen vernetzte Geräte und IoT-Devices Sicherheitsschwierigkeiten, weil sie unzureichende Security-Features besitzen und nicht über Update-fähige Betriebssysteme verfügen.

Doch in der Medizintechnik wird die Situation dadurch noch komplexer, dass Medizingeräte nicht mehr verändert werden dürfen, sind sie einmal zertifiziert.

Dies schließt auch das Betriebssystem oder eine Antiviren-Software ein.

Aufgrund der fortschreitenden IP-Vernetzung unterliegen sie zugleich den gleichen Sicherheitsrisiken wie klassische IT-Endpoints, etwa PCs oder Server.

Viele IoMT-Devices werden obendrein innerhalb der Einrichtungen als mobile Endgeräte genutzt, so dass sie über verschiedene Zugangspunkte ins Netzwerk gehen und nicht ohne weiteres separiert werden können.

Niemand kann davon ausgehen, dass heutige vernetzte Medizintechnik gegen Angriffe von morgen gewappnet ist.

Die connected Things bieten somit ein mögliches Einfallstor für Hacker und eine sehr große Angriffsfläche. PwC schreibt in seiner Studie „Global Top Health Industry Issues“: „Je häufiger ans Internet angeschlossene medizinische Geräte und Netzwerke im Gesundheitswesen verwendet werden, desto höher ist das Risiko, dass sie zum Ziel von Cyberattacken, Ransomware und Malware werden. Dabei stehen vor allem sensible Patientendaten im Fokus.“ [2]

6. HOHER VIRTUALISIERUNGSGRAD

Wenn Hunderte von Mitarbeitern Zugriff auf sensiblen Daten benötigen, kommt dafür in der Regel eine Virtual Desktop Infrastructure (VDI) zum Einsatz.

So auch in vielen Healthcare-Einrichtungen: Die Mitarbeiter benutzen PCs, Thin Clients, Laptops oder Tablets, doch die Nutzer-Sessions laufen nicht auf dem Endgerät, sondern im Rechenzentrum. Dort bleiben alle Daten.

Nur Bildschirmupdates werden an die Endgeräte gestreamt. Ärzte, Pfleger und Verwaltungspersonal haben bequemen Zugriff auf die Daten, für die sie berechtigt sind – zum Beispiel im Krankenhausinformationssystem (KIS) - laden diese Daten aber nicht auf ihre Endgeräte herunter.

Dies bietet viele Vorteile hinsichtlich Datenschutz, Netzwerksegmentierung und Data Leak Prevention. Es ermöglicht einen zentralisierten, hochgradig effizienten IT-Betrieb mit einer geringen Angriffsfläche auf die genannten klassischen IT-Endpoints.

Auch beim Betrieb von Servern ist Virtualisierung längst der Regelfall im Gesundheitswesen. Eine hundertprozentig virtualisierte IT-Umgebung aus einem Guss wäre verhältnismäßig leicht zu managen und zu sichern. Die Krux ist, dass dies in dieser Reinheit nie der Fall ist.

Durch Legacy-Systeme, vernetzte Medizingeräte, besondere Umstände wie Fusionen, und wegen einzelner Anwender und Endgeräte mit besonderen Ansprüchen besteht die IT-Umgebung immer aus einem Mix aus einer oder mehreren Virtualisierungsumgebungen, klassischer IT und neuartigen Geräten.

Diese heterogene IT-Umgebung erfordert verschiedene Schutzmechanismen. An diesem Punkt kann der Schutz aufwändig und komplex werden. Oder löchrig: In der Praxis scheitern viele Einrichtungen des Gesundheitswesens bereits daran, die IT vollständig zu inventarisieren und zu dokumentieren.

Bitdefender

7. KOSTENDRUCK

Selbst IT-Leiter sehen ihre Krankenhäuser selten auf dem neuesten Stand der IT-Technik. Sprichwörtlich ist der Einsatz von Windows-XP-Rechnern für bestimmte Zwecke, obwohl diese als sehr unsicher gelten und der Support längst eingestellt ist.

Dies illustriert den enormen Kostendruck in der Branche. Einrichtungen des Gesundheitswesens haben stark regulierte Vorgehensweisen, die sie einhalten müssen und nur geringe Möglichkeiten, ihre Umsätze zu erhöhen.

Laut der Unternehmensberatung Roland Berger konnten im Jahr 2017 41 Prozent der Krankenhäuser keinen Überschuss erwirtschaften. [6]

Für das Geschäftsjahr 2018 gingen sie von einer weiteren Verschlechterung ihrer wirtschaftlichen Situation aus.

Eine Arbeitsgruppe zum Thema „Cyber Security“ im Jahr 2016 kam ebenfalls zu dem Schluss, dass mangelnde Investitionen in neue IT-Systeme zu den größten Stolpersteinen für eine sichere IT gehören. [7]

Durch die KRITIS-Anforderungen sind in einigen Häusern Investitionen in die IT-Sicherheit unumgänglich geworden.

Laut einer Befragung des Meinungsforschungsinstitut Censuswide seien zuletzt immerhin bei 40 Prozent der 150 deutschen befragten IT-Fachkräfte im Gesundheitswesen die verfügbaren finanziellen Mittel für IT-Sicherheit um 11-20 Prozent gestiegen. [8]

Das Fazit bleibt jedoch: Obwohl nur mithilfe eine umfassenden Digitalisierung die Möglichkeit besteht, unter heutigen Voraussetzungen im Healthcare-Bereich effizient und auf Dauer kostendeckend oder mit Gewinn zu arbeiten, fehlen den Einrichtungen die Mittel, um diese notwendigen Investitionen zu tätigen.

Bitdefender

IT-SICHERHEITSRISIKEN IM GESUNDHEITSWESEN

Bitdefender

Gesundheitseinrichtungen sind beliebte Ziele von Cyberkriminellen. Diese wissen nicht nur um den Wert von Gesundheitsdaten. Sie wissen auch, wie eng eine funktionierende IT und Datenzugang mit dem Patientenwohl verknüpft sind, und dass schon ein um wenige Minuten verzögerter Prozess irreversible Gesundheitsschäden bedeuten kann.

Viele Länder haben den Gesundheitssektor schneller als Deutschland digitalisiert. Zugleich haben sie weniger Rücksicht auf IT- und Datensicherheit genommen. Entsprechend viele Beispiele für folgenreiche Attacken gibt es. Auch in Deutschland mit dem vergleichsweise niedrigen Digitalisierungsgrad und hohen Sicherheitsvorkehrungen sind Vorfälle bekannt (siehe Kasten). Die Dunkelziffer dürfte hoch sein, da eine umfassende Meldepflicht erst seit kurzem greift.

Vor allem drei Angriffstypen sind gängig:

1. **Erpressung**
2. **Einfall über ungeschützte Medical Things**
3. **Gezielter Datendiebstahl**

Bitdefender

1. ERPRESSUNG

Mit Ransomware verschlüsseln Cyberkriminelle Daten und verlangen ein Lösegeld für das Passwort zur Entschlüsselung.

In der Vergangenheit waren Praxen, Pflegeeinrichtungen, Unternehmen und Krankenhäuser oft Opfer von gestreuten Ransomware-Kampagnen. Das heißt, Angreifer versuchten, möglichst viele Opfer in kurzem Zeitraum zu erreichen.

Die Opfer waren oft zufällig und die Lösegeldforderungen hatten nur den Wert einiger hundert Euro. In Zukunft wird erwartet, dass kriminelle Organisationen Ransomware zunehmend gezielt nutzen, um ausgewählte Unternehmen und Einrichtungen um einen weitaus höhere Betrag zu erpressen.

Auch andere Wege der digitalen Erpressung, etwa über die direkte Kontrolle von Servern und Netzwerkkomponenten oder DDoS-Angriffe, gehören zu den Szenarien, für die sich der Healthcare-Sektor wappnen muss.

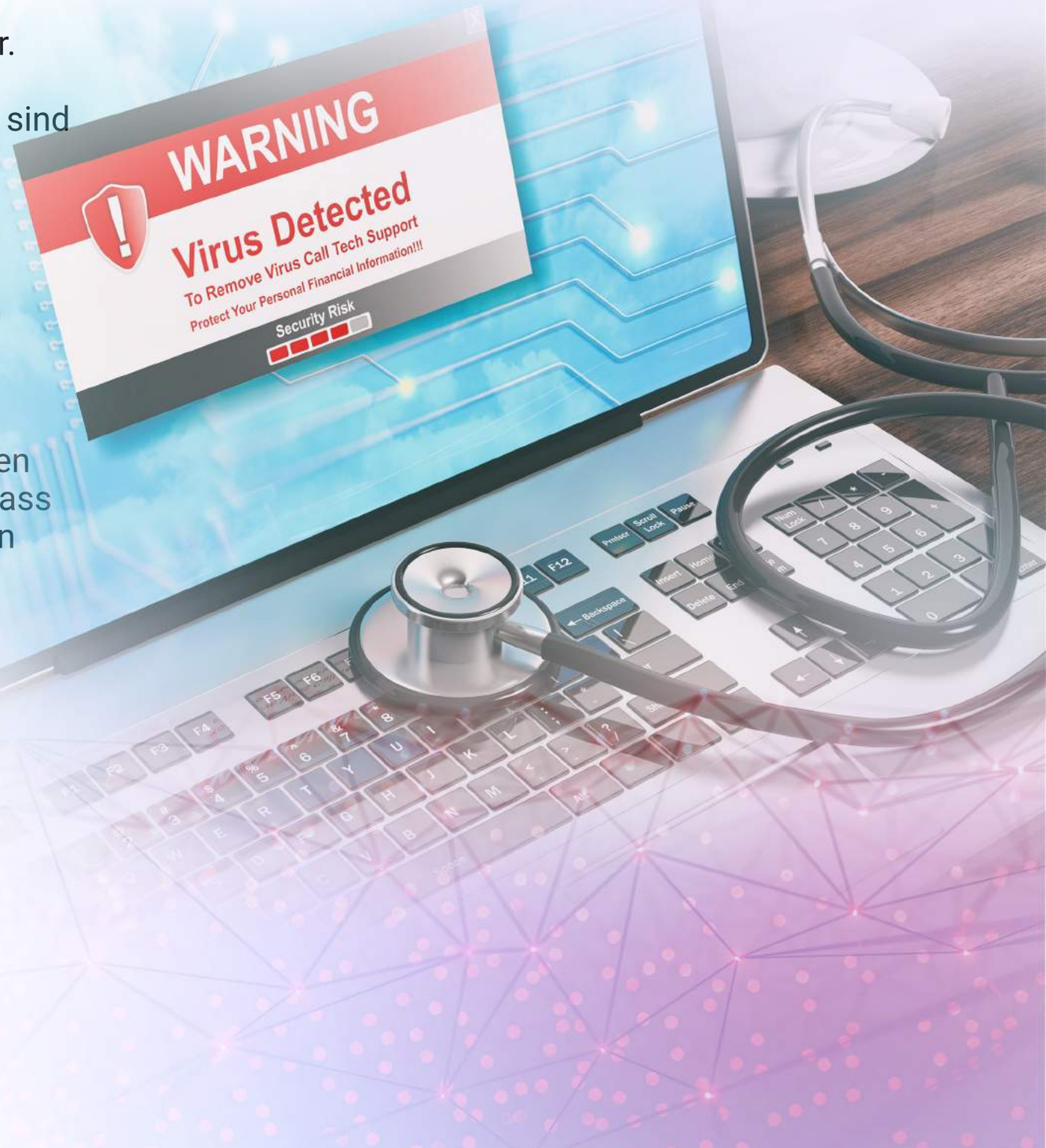
2. EINFALL ÜBER UNGESCHÜTZTE MEDICAL THINGS

Medical Things sind prädestinierte Einfallstore für Hacker.

Selbst wenn sie über bekannte Schwachstellen verfügen, sind Betreibern und Herstellern die Hände gebunden, sie zu aktualisieren, weil sie damit die Zertifizierung verlieren würden.

Angesichts der großen und weiter steigenden Menge von Geräten, ist es somit eine eher leichte Übung für Hacker, Kontrolle über ein unsicheres Gerät zu erlangen.

IT-Sicherheitsbeauftragte stehen somit vor der schwierigen Herausforderung, die vernetzten Things so zu isolieren, dass Hacker die IoMT-Geräte möglichst gar nicht erst auffinden können und sich ansonsten nicht zu sensiblen Daten und weiteren Geräten vorarbeiten können.



3. GEZIELTER DATENDIEBSTAHL

Wenn es den Angreifern vor allem darum geht, Daten zu erbeuten, gibt es viele Wege. Dazu spähen Cyberkriminelle ihre Opfer in vielen Fällen über längere Zeit gezielt aus, um alles über die Netzwerkkonfiguration, Richtlinien, Zugänge und intern eingesetzte Sicherheitslösungen herauszufinden.

Am häufigsten beginnt eine solche Attacke über Spear-Phishing, also raffinierte Emails, die wegen Insider-Informationen einen legitimen Eindruck erwecken.

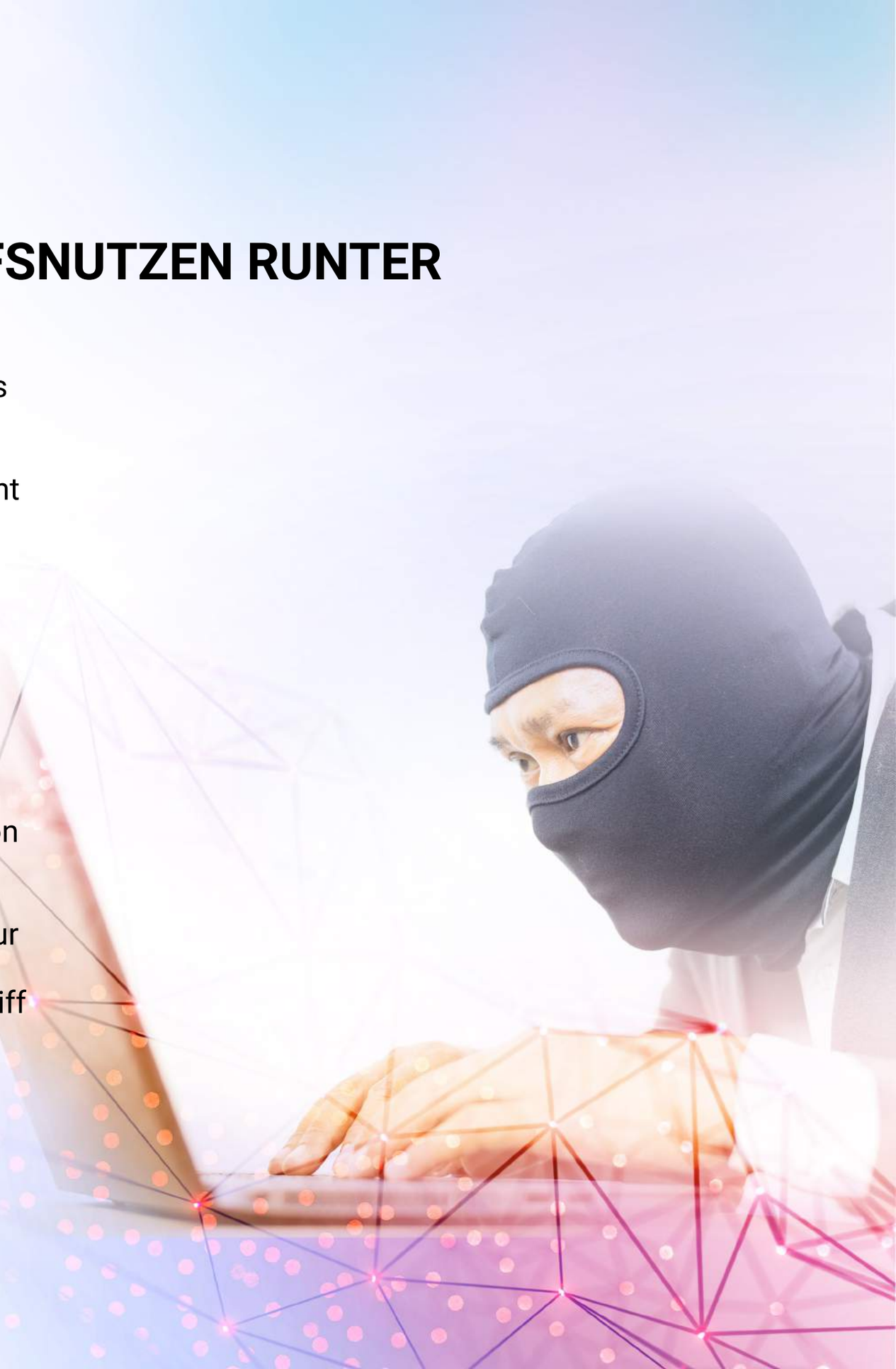
Oft hat ein Angriff mehrere Stufen, in denen die Hacker neue Schwachstellen ausnutzen, Identitäten stehlen und missbrauchen, verschiedenste Malwares (inklusive dateiloser Malware) und Hacking-Techniken wie Code Injection oder Function Detouring eingesetzen. Die Königsdisziplin sind Advanced Persistent Threats (APTs): Diese bleiben im schlimmsten Fall jahrelang unentdeckt und ermöglichen Cyberkriminellen über lange Zeit hinweg, umfangreiche Datenmengen zu stehlen und geben ihnen dauerhaft Zugriff auf sensible Dateien.

ANGRIFFSKOSTEN HOCH, ANGRIFFSNUTZEN RUNTER

Die Waffen der Cyberkrimininellen sind also vielfältig, daher müssen auch die Abwehrmechanismen vielschichtig sein. Es braucht nicht einen Schutzschirm, sondern viele Sicherheitsschichten. Ein herkömmlicher Antivirus und eine Firewall gehören zur Grundausstattung, doch sie reichen nicht aus.

Wie macht man Cyberkriminellen das Leben schwer? Im Prinzip ist es einfach: Man erhöht die Hürden um ein Vielfaches und man reduziert den möglichen Nutzen für die Hacker auf einen Bruchteil. Es geht darum, dass es richtig anstrengend wird für die Kriminellen, an ihr Ziel zu kommen und sie dann dennoch mit leeren Händen dastehen, zum Beispiel weil sie wertlose oder verschlüsselte Daten erhalten oder weil der Angriff unmittelbar nach dem Beginn Exfiltration gestoppt wird.

In der Sprache der Security-Spezialisten geht es also nicht nur um die Pre-Execution-Phase, sondern auch um die On-Execution- und Post-Breach-Phase. Selbst wenn ein Angriff nicht verhindert werden konnte, ist oft noch Gelegenheit, ihn zu stoppen und die Folgen zu minimieren.



Bekannte Sicherheitsvorfälle im Gesundheitswesen

Februar 2017: Das **Lukaskrankenhaus in Neuss** wird von Ransomware befallen und kann daraufhin einige Zeit keine Notfälle auf und verschiebt Operationen. Die Klinik geht vorbildlich transparent mit dem Vorfall um und beziffert die Kosten später auf 1 Million Euro. [9]

August 2017: Nach einem Malware-Angriff auf die **britische Gesundheitsbehörde NHS** in der Grafschaft Lankarshire werden die 655.000 Bewohner aufgefordert, nur in wirklichen Notfällen die drei Krankenhäuser aufzusuchen. Unter anderem waren die Telefonanlagen und Verwaltungssoftware ausgefallen. [10]

2010 bis 2017: Laut einer im Journal of the American Medical Association veröffentlichten Studie sind in den **USA** von 2010 bis 2017 über **176 Millionen Patientendaten** von irgendeiner Form von Sicherheitsvorfall betroffen. [11]

November 2018: Der Trojaner Emotet legt das **Krankenhaus Fürstenfeldbruck** bei München lahm. Krankenwagen können die Klinik elf Tage lang nicht anfahren. [12]

Februar 2019: In Singapur gelangen über eine zentrale Datenbank die **Namen von 14.000 HIV-Patienten** an die Öffentlichkeit. [13]

Bitdefender

VIELSCHICHTIGER SCHUTZ

Weder ein herkömmlicher Antivirus, noch Firewalling noch irgendeine andere Technologie kann alleine eine umfassende Sicherheit bieten. Es ist wie im Flugverkehr: Auch dort müssen viele Schutzmechanismen ineinandergreifen. Bestandteile des Sicherheitskonzepts sind unter anderem Passagierdatenkontrolle, Gepäckkontrolle, Metallsensoren, Passkontrolle, Video-Überwachung, Polizeipräsenz, Mitarbeitertraining, Alarmsysteme, Notfallpläne und vieles mehr.

So benötigt auch der Schutz einer modernen IT-Umgebung viele Schichten. Für Angreifer bedeuten diese Schichten, dass sie in ihren Angriffen viele Umwege in Kauf nehmen und viel mehr Zeit einsetzen müssen. Sie müssen eine Hürde nach der anderen nehmen - jede höher als die vorherige - , um an ihr Ziel zu kommen und immer in dem Bewusstsein, dass die bisherigen enormen Anstrengungen umsonst sein könnten, wenn sie an der nächsten Sicherheitsschicht scheitern. Cyberkriminelle denken wirtschaftlich: Sie werden den Angriff aufgeben, wenn das erreichbare Ziel den Aufwand nicht mehr rechtfertigt.

Einige wichtige Schichten einer modernen IT-Security im Healthcare-Bereich sind untenstehend beschrieben:

1. **Next Gen Anti-Malware**
2. **Endpoint Detection and Response (EDR)**
3. **Network Traffic Security Analytics (NTSA)**

Bitdefender

1. NEXT GEN ANTI-MALWARE

Herkömmliche Endpoint Security ist unverzichtbar und leistet bereits viel: Gängige Antivirus-Lösungen wehren weit über 99 Prozent aller Malware-Angriffe ab.

Ein zeitgemäßer Schutz von Endgeräten benötigt jedoch neue Features.

Dazu gehören der automatisierte Vergleich von noch unbekannten Dateien zu bekannten bösartigen und legitimen Dateien.

Weitere Ebenen sind die Machine-Learning gesteuerte HyperDetection, die auch bösartige dateilose Befehle und Skripte einschließlich VB-, JAVA-, PowerShell- und WMI-Skripte prüft, und das Sandboxing, in dem verdächtige Dateien in einer isolierten Umgebung geöffnet und beobachtet werden.

Unverzichtbar ist die Überwachung aller laufender Prozesse auf den Engeräten, um festzustellen, ob Unregelmäßigkeiten auftreten oder ob andere Prozesse manipuliert werden.

Diese neuen hochmodernen Features werden als Next Generation Security bezeichnet. Doch aufgepasst: Viele sogenannte NextGen Tools sind aber bloße One-Trick Ponys, mit einem extrem schmalen Funktionsumfang - zum Beispiel nur Malware-Erkennung auf der Basis eines einzigen Machine-Learning Algorithmus.

Wer seine Sicherheit maximieren will, ohne den Aufwand zu vervielfachen, benötigt eine konsolidierte Lösung aus herkömmlichem Antivirus und den vielen Next-Gen-Funktionen.

2. ENDPOINT DETECTION AND RESPONSE (EDR)

Endpoint-Security-Tools hatten in der Vergangenheit ihren Fokus nur auf der „pre-execution“ Phase. D.h. die Augabe bestand darin, Angriffe zu verhindern.

Erst seit einigen Jahren reagieren sie mittels Next-Gen-Features auch „on-execution“ und unterbinden illegitime Prozesse unmittelbar nachdem diese gestartet wurden, etwa ein Verschlüsselungsprozess durch zuvor unbekannte Ransomware. Dem gegenüber kommt EDR (Endpoint Detection and Response) „post-breach“ ins Spiel. Dies ist notwendig, denn nicht jeder ausgeklügelte Angriff lässt sich vorab erkennen.

Man kann sich Endpoint Security als eine Mauer vorstellen. Sobald diese durchbrochen ist, kann sie nichts mehr ausrichten. Dann müssen andere Tools greifen, die eher einer Polizeistreife oder einem Ermittlungsteam ähneln, das die grenznahen Bereiche durchforstet und überwacht.

EDR-Tools entdecken verdächtige Aktivitäten auch zu einem späteren Zeitpunkt automatisch und alarmieren gegebenenfalls IT- und Sicherheitsteams über Ungereimtheiten.

Bitdefender

Um den Aufwand für IT-Verantwortliche zu minimieren, sollten Endpoint Security und EDR miteinander zusammenarbeiten.

So können sie Informationen über potenzielle Sicherheitsprobleme austauschen und alle für Sicherheits- und IT-Administratoren relevanten Informationen in einer einzigen zentralen Managementkonsole anzeigen.

Um Alarmmüdigkeit vorzubeugen, ist eine Schlüsselkomponente von EDR der nächsten Generation ein intelligentes Scoring der Sicherheitsvorfälle auf Basis von Machine Learning.

Administratoren erhalten auf diese Weise einen vollständigen Überblick über den Sicherheitsstatus der Infrastruktur des Unternehmens und werden nicht durch eine Fülle von Warnmeldungen mit niedriger Priorität lahmgelegt.

Bitdefender

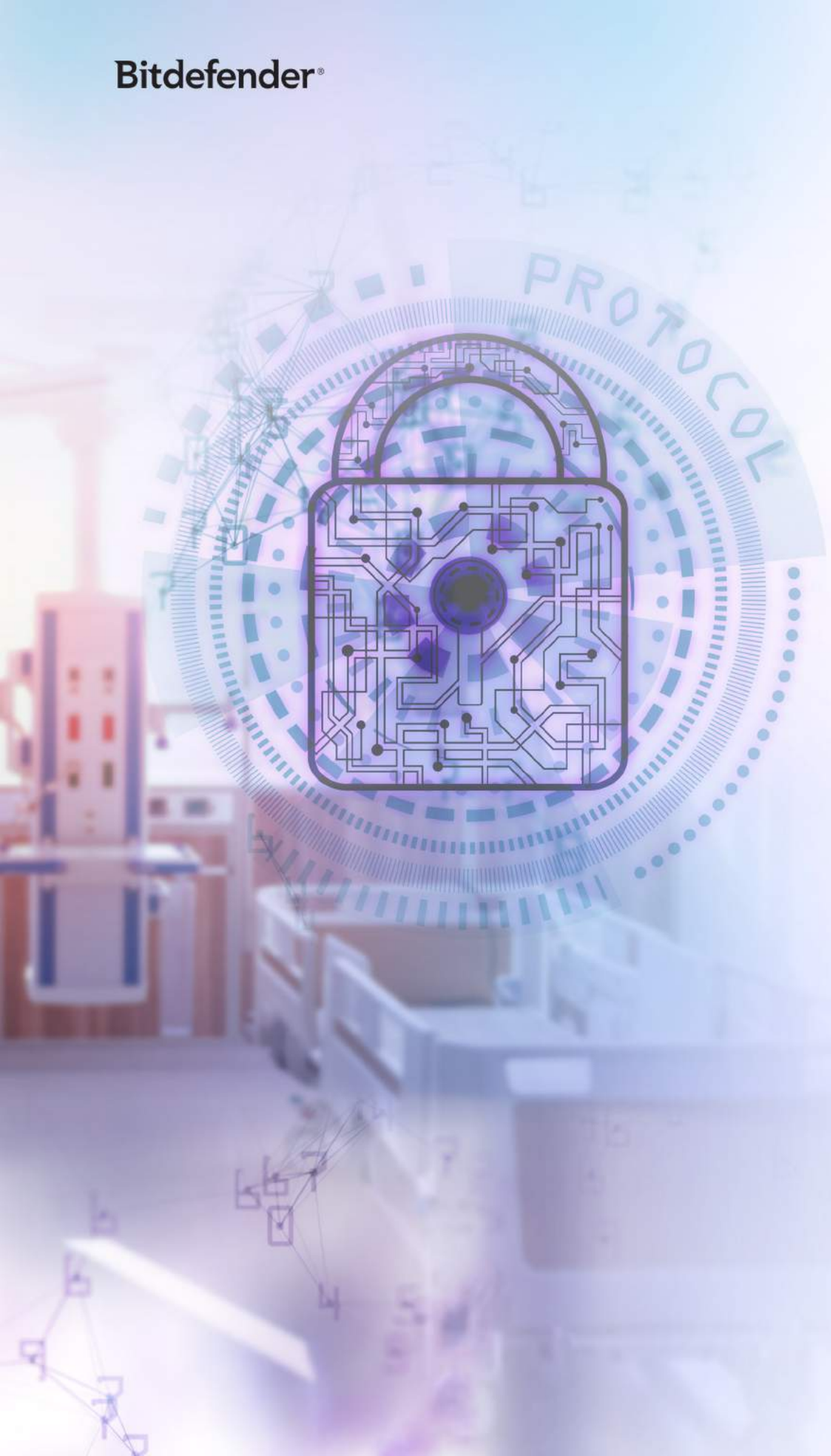
3. NETWORK TRAFFIC SECURITY ANALYTICS (NTSA)

Kriminelle, die Advanced Persistent Threats (APTs) lancieren, verwenden höchsten Aufwand darauf, dass die entscheidenden Vorgänge beim digitalen Einbruch einen legitimen Anschein erhalten.

Dies gelingt ihnen zum Beispiel, indem sie reale Nutzernamen und Passworte von Administratoren oder Topmanagern phishen. ein anderer Weg ist es, noch unbekannte Schwachpunkte legitimer Anwendungen zu missbrauchen und die eigenen Spuren nach gelungenem Einbruch in die IT-Systeme wieder zu löschen.

Derzeit gängige Sicherheitslösungen erkennen solcherart getarnte Angriffe nicht. Nur durch eine intelligente Analyse des Netzwerk-Traffics (Network Traffic Security Analytics, NTSA) lassen sich APTs identifizieren. Eine NTSA-Lösung erlernt das typische Verhalten im Netzwerk und erkennt dadurch Abweichungen.

NTSA ergänzt Abwehrmaßnahmen wie Firewalling und Endpoint Security, weil sie etwas hat, das kein anderes Sicherheitstool hat: Detaillierte Kenntnisse über das typische Verhalten jedes Endpunkts aus Netzwerksicht.



Jeder APT hinterlässt Spuren im Netzwerk, die sich anhand von Netzwerk-Metadaten nachverfolgen lassen. Wer Daten exfiltrieren will, muss sie zu guter Letzt irgendwann im Netzwerk bewegen.

NTSA stützt sich auf Metadaten, um detaillierte Kenntnisse über das Verhalten jedes Endpunkts im Netzwerk zu liefern und anomales Verhalten zu entlarven. Aus sicherheitstechnischer Sicht schließt die Netzwerk-Traffic-Analyse die Lücke zwischen Next-Gen-Firewalls und IDS/IPS und ergänzt Netzwerküberwachung und EDR (Endpoint Detection&Response).

NTSA nutzt Künstliche Intelligenz sowie Verhaltens- und Bedrohungsanalyse, um ausgefeilte Bedrohungen zu erkennen. Sie speichert Metadaten für zur nachträglichen Erkennung von Bedrohungen, also Forensik und Compliance.

NTSA ist für den Gesundheitsbereich nicht zuletzt deshalb bestens geeignet, weil diese Technologie mit Metadaten arbeitet und für die Analysen keine Sichtbarkeit sensibler Patientendaten benötigt.

Bitdefender

KONSOLIDIERUNG UND AUTOMATISIERUNG DER IT-SICHERHEIT

Bitdefender

Cybersicherheit erfordert täglich mehr Know-How, während der Arbeitsmarkt für IT-Sicherheitsspezialisten leergefegt ist. Vor diesem Hintergrund sollten Unternehmen jegliche Chance zur Sicherheitsautomatisierung nutzen.

Zum Beispiel sorgt ein System für Entlastung, das neu geschaffene virtuelle Endpunkte garantiert von der ersten bis zur letzten Sekunde schützt. Das gleiche gilt für ein EDR, das mit der Endpoint Protection Platform Informationen austauscht, Sicherheitsvorfälle anhand eines Scores priorisiert und Vorschläge zur Remediation per Mausklick anbietet. Je mehr Funktionen konsolidiert und übersichtlich zur Verfügung gestellt werden, und je mehr Automatisierung die Managementoberfläche bietet, desto besser unterstützt die Lösung die besonderen Herausforderungen der Healthcare-Branche.

Grundlegend ist dafür, dass der Schutz der omnipräsenten virtuellen Systeme mit dem aller anderen Systeme integriert und konsolidiert ist. Viele Organisationen im Healthcare-Sektor greifen heute für den Schutz virtueller Systeme auf komplett andere Produkte zurück, als für ihre physische Hardware. Dies verursacht erhebliche Mehrkosten in der Administration.

Sinnvoll ist ein einheitliches System, das sowohl physische als auch virtuelle Endpoints einheitlich von einer Management-Oberfläche verwaltbar macht. Eine solche Lösung benötigt einen universal einsetzbaren Agenten für alle Betriebssysteme und Hypervisoren.

Bitdefender

Nur wenn eine Organisation sicherstellen kann, dass jeder virtuelle Endpunkt schon von Sekunde eins gesichert ist und während seines gesamten Lebenszyklus geschützt bleibt, erhält sie eine sichere Umgebung.

Die heute üblichen Sicherheitstechnologien sind im besten Fall bereits darauf ausgelegt, physische und virtuelle Endpunkte von einer einheitlichen Konsole aus zu sichern. Doch fast immer verwenden sie den Full-Agent Ansatz. Das heißt, ein Host mit 1.000 virtuellen Maschinen benötigt auch 1.000 Agents für die Endpoint-Sicherheit. Die Sicherheit kann bis zu 20 Prozent der Performance schlucken. Um Prozessor-Power der virtuellen Systeme zu schonen, ist ein im Rechenzentrum zentralisierter, agentenloser Schutz ideal, dann findet das Malware-Scanning zentralisiert auf Hypervisor-Ebene statt.

Virtualisierung lässt sich noch für eine weitere Sicherheitsschicht nutzbar machen. Dieser Ansatz, getauft Hypervisor Introspection (HVI), setzt IT-Sicherheit erstmals von der Hypervisor-Ebene aus durch und blockiert ausgefeilte Attacken agentenlos und von außerhalb des Betriebssystems durch Überwachung des Arbeitsspeichers. Aus Sicht der Angreifer ist Hypervisor Introspection wie eine unsichtbare Schutzwand: Sie können sie nicht sehen und bemerken nur, dass die illegitimen Prozesse wieder und wieder geblockt werden.

Bitdefender

ZUSAMMENFASSUNG: DIGITALISIERUNG ERMÖGLICHEN

Bitdefender

Kennzeichnend für die IT-Security-Herausforderung des Healthcare-Sektors sind die hohe Sensibilität der Daten und die Notwendigkeit mit begrenzten Mitteln und Ressourcen, dem Vertrauen der Patienten und den hohen Compliance-Anforderungen gerecht zu werden.

Dass die Wertschöpfungskette und die Datenerfassung im Gesundheitsbereich digitalisiert werden muss, steht nicht in Frage, da nur so auf Dauer kostendeckend oder mit Gewinn gewirtschaftet werden kann.

IT-Sicherheit ist dabei eine Vorbedingung, die erfüllt sein muss: Daten müssen erhalten bleiben und gegen den Zugriff von außen geschützt bleiben.

Der Patient muss jederzeit Vertrauen haben, dass seine Intimsphäre geschützt bleibt.

Die Gefahren, die durch Hacker und kriminelle Organisationen drohen, sind dabei immens, wie zahlreiche Vorfälle belegen, und die Angriffswege sind vielfältig. Notwendig ist daher ein vielschichtiger Schutz.

Dazu gehören Funktionen für den Pre-Execution-Schutz, die Angriffsunterbindung on-execution und Post-Breach-Tools zur Minimierung von Angriffsfolgen und Aufklärung, insbesondere Next Generation Anti-Malware, Endpoint Detection&Response (EDR) und NTSA. Sie erhöhen die Kosten für die Angreifer und reduzieren ihren möglichen finanziellen Gewinn. Eine Sicherheitsinfrastruktur aus Einzellösungen würde die oft kleinen IT-Teams schnell überfordern.

Konsolidierte Lösungen und Automatisierung helfen dagegen dabei, im Gesundheitswesen trotz Kostendrucks bei der IT-Sicherheit den heutigen Stand der Technik vollumfänglich umzusetzen und schnell die Produktivitätsgewinne der Digitalisierung einzufahren.

Bitdefender

Bitdefender GravityZone

GravityZone ist eine umfassende und integrierte Suite von Security-Lösungen für Organisationen und Unternehmen. Zu den Vorteilen für das Gesundheitswesen gehören diese Punkte:

- Einheitliches, übersichtliches Management über alle Funktionen und Endpunkte hinweg
- Vielschichtiger Schutz inklusive Next Generation Security
- Universeller Software-Agent für alle Betriebssysteme, virtuelle Systeme und Cloud-Instanzen
- Agentenloser Schutz von virtuellen Systemen (Central Scanning und HVI)
- Einheitliche Lizenzierung unabhängig von der Art des Endpunkts
- Günstige Lizenzierung nach CPUs für virtuelle Systeme
- EPP, EDR und NTSA in einer Geamtlösung
- Anti-Malware-Engine, die seit Jahren durchgehend Topbewertungen der führenden Testinstitute AV-Test und AV-Comparatives erhält
- Produkt aus der EU
- Hochgradig automatisierte Administration und Bereinigung von Sicherheitsvorfällen
- Voll DSGVO- und KRITIS-konform

Bitdefender

KONTAKT

„Sie arbeiten in einem Unternehmen des Healthcare-Sektors und wollen Ihre IT-Sicherheit auf den aktuellen Stand der Technik bringen? Bitdefender hat die richtigen Lösungen und bietet einzigartige Möglichkeiten, ihre IT effizient abzusichern. Gerne beraten wir Sie und stellen unsere Lösungen in einem Proof of Concept vor. Kontaktieren Sie uns.“

Thomas Krause, Regional Sales Director Enterprise DACH, Bitdefender

Thomas Krause
Regional Sales Director Enterprise DACH
Telefonnummer
E-Mail
Adresse

Über Bitdefender

Bitdefender ist ein weltweit führender Anbieter von Cybersicherheitslösungen und Antivirensoftware und schützt über 500 Millionen Systeme in mehr als 150 Ländern. Seit der Gründung im Jahr 2001 sorgen Innovationen des Unternehmens regelmäßig für ausgezeichnete Sicherheitsprodukte und intelligenten Schutz für Geräte, Netzwerke und Cloud-Dienste von Privatkunden und Unternehmen. Als Zulieferer erster Wahl befindet sich Bitdefender-Technologie in 38 Prozent der weltweit eingesetzten Sicherheitslösungen und genießt Vertrauen und Anerkennung bei Branchenexperten, Herstellern und Kunden gleichermaßen.
www.bitdefender.de

Bitdefender

QUELLEN

[1] McKinsey: September 2018, „Digitalisierung im Gesundheitswesen: die Chancen für Deutschland“, https://www.mckinsey.de/~/media/mckinsey/locations/europe%20and%20middle%20east/deutschland/news/presse/2018/2018-09-25-digitalisierung%20im%20gesundheitswesen/langfassung%20digitalisierung%20im%20gesundheitswesen__neu.ashx

[2] PwC, 5. November 2018, „Studie ‚Global Top Health Industry Issues‘: PwC beleuchtet die acht wichtigsten Trends im weltweiten Gesundheitswesen“, https://www.pwc.de/de/pressemitteilungen/2018/studie-global-top-health-industry-issues-pwc-beleuchtet-die-acht-wichtigsten-trends-im-weltweiten-gesundheitswesen.html

[3] Bundesgesundheitsministerium, E-Health-Initiative, Juni 2019, https://www.bundesgesundheitsministerium.de/e-health-initiative.html

[4] Roland Berger, Juli 2017, „Roland Berger Krankenhausstudie 2017“ https://www.rolandberger.com/de/Publications/Krankenhausstudie-2017.html

[5] Frost&Sullivan, Juni 2017, „Internet of Medical Things, Forecast to 2021”, https://store.frost.com/internet-of-medical-things-forecast-to-2021.html

[6] Roland Berger, Juni 2018, „Roland Berger Krankenhausstudie 2018“, https://www.rolandberger.com/publications/publication_pdf/roland_berger_krankenhausstudie_2018.pdf

[7] HIMSS D-A-CH Community, April 2016, "DACH Community Frühstück: Interaktiv, progressiv und konstruktiv" https://www.eiseverywhere.com/ehome/158577/april2016/

[8] IT-Daily.net (Pressmitteilung von Infoblox), "KRITIS-Verordnung IT-Security: Umdenken an deutschen Krankenhäusern", 06. Juni 2019, https://www.it-daily.net/analysen/21586-it-security-umdenken-an-deutschen-krankenhaeuser

[9] heise.de, 05. Februar 2017, „Trojaner im OP - wie ein Krankenhaus mit den Folgen lebt“, https://www.heise.de/newsticker/meldung/Trojaner-im-OP-wie-ein-Krankenhaus-mit-den-Folgen-lebt-3617880.html

[10] heise.de, 8. August 2017, „Malware-Angriff auf britische Gesundheitsbehörde“, https://www.heise.de/newsticker/meldung/Malware-Angriff-auf-britische-Gesundheitsbehoerde-3813736.html

[11] Reuters, 25.09.2018, „Health data breaches on the rise” https://www.reuters.com/article/us-health-data-security/health-data-breaches-on-the-rise-idUSKCN1M524J

[12] Bayrischer Rundfunk, 23.01.2019, „Hackerangriff: Wenn Krankenhäuser lahmgelegt werden“, https://www.br.de/nachrichten/deutschland-welt/hackerangriff-wenn-krankenhaeuser-lahmgelegt-werden

[13] Bayrischer Rundfunk, 30.05.2019, „Sicherheitslücken: Probleme mit der elektronischen Patientenakte“, https://www.br.de/nachrichten/deutschland-welt/sicherheitsluecken-probleme-mit-der-elektronischen-patientenakte,RRmEPve