PHILIPS

Services and Solutions Delivery

Operative Intelligenz

Unternehmensweite Cybersicherheit

Executive Briefing

Unternehmensweite Cybersicherheit

„Cybersicherheit steht beim Übergang zur vernetzten Versorgung im Mittelpunkt."
Jeroen Tas, Chief Innovation & Strategy Officer, Philips

Angriffe auf Betriebstechnik (Operational Technology, IoT-Geräte) stiegen jedes Jahr um **2.000 %** an. Bedrohungsakteure verlagern ihr Augenmerk weiterhin auf Angriffsvektoren wie IoT-Geräte und vernetzte industrielle und medizinische Systeme.

8,5 Milliarden betroffene Datensätze im Jahr 2019, wodurch Angreifer Zugang zu mehr gestohlenen Anmeldedaten erhielten. Die Sicherung von Anmeldedaten und Zugriffskontrollen ist wichtiger denn je.

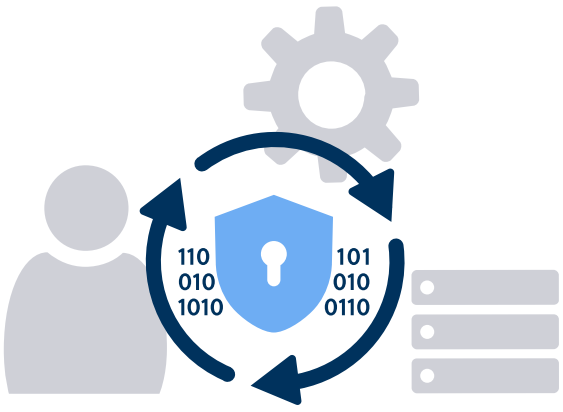
150.000 Schwachstellen bis dato offen gelegt. Das Schließen von Schwachstellen ist für viele Unternehmen immer noch ein Problem, und Cyberkriminelle wissen das.

Quelle: IBM X-Force Threat Intelligence Index 2020

Bei so vielen komplexen "Quadruple aim"-Anforderungen an die Geschäftsführung neigen viele Organisationen im Gesundheitswesen dazu, die Verantwortung für die Cybersicherheit den technischen Experten zu überlassen, in der Annahme, dass der CIO (IT-Leiter) oder CISO (IT-Sicherheitsbeauftragter), falls es einen gibt, die Verantwortung übernehmen wird. Und dennoch haben viele CIOs oder CISOs nur einen begrenzten Teil des Unternehmens im Blick, sodass das Wissen auf Unternehmensführungsebene und die Budgetzuweisung entscheidend sind.

Das Gesundheitswesen war laut IBM Security X-Force in 2020 an siebter Stelle der von Cyberkriminellen bevorzugten Branchen. Leitende Führungskräfte wie CEOs und COOs, deren Aufgabenbereich die gesamte Organisation umfasst, sind in einer wichtigen Position, um den notwendigen Wandel voranzutreiben und unternehmensweite Cybersicherheit zu entwickeln und einzusetzen. In der Tat muss das Engagement für eine effektive Cybersicherheit horizontal sein und Silo-Denken aufbrechen, um eine kontinuierliche Zusammenarbeit zwischen dem medizinischen Betrieb und dem technischen Personal zu schaffen.

In dieser kurzen Lektüre gehen wir auf das notwendige Wissen und die notwendigen Handhabungen für das Management der Cybersicherheit im Gesundheitswesen auf Führungsebene ein, stellen die Schlüsselfragen, die sich alle leitenden-Fürungskräfte stellen müssen, und geben wichtige Tipps zur Vermeidung von Datenschutzverletzungen und Cybersicherheitsbedrohungen im Gesundheitswesen.



Cybersicherheitsmanagement und Organisationen im Gesundheitsbereich

Mit dem Gesundheitswesen an siebter Stelle der von Cyberkriminellen bevorzugten Branchen, benennen wir die 5 wichtigsten Erkenntnisse zur Vermeidung von Datenschutzverletzungen und Cybersicherheitsbedrohungen im Gesundheitswesen.

Erkenntnis 1:
Nicht mehr allein Technik

Erkenntnis 2:
Beziehungen und Zusammenarbeit sind der Schlüssel

Erkenntnis 3:
Wissen aneignen und die richtigen Fragen stellen

Erkenntnis 4:
Für den schlimmsten Fall planen

Erkenntnis 5:
Sprechen Sie mit Philips über unsere branchenführenden Cybersicherheits-lösungen

Erkenntnis 1: Nicht mehr allein Technik. Cybersicherheit ist eine sich entwickelnde, komplexe betriebliche Herausforderung.
Das Aufkommen des Internets und der Interkonnektivität hat viele ehemals geschlossene Netzwerke innerhalb von Krankenhäusern geöffnet und birgt für diese neue Risiken. Veraltete IT-Ausstattung und auch veraltete Sicherheitsmaßnahmen – Passwörter, Verschlüsselung und andere Maßnahmen – entsprechen möglicherweise nicht dem erforderlichen Standard für die heutige IoT-Welt.

Leistungserbringer sehen sich außerdem mit einem ernsthaften Mangel an qualifizierten IT-Fachkräften, die mit Cyberangriffen[1] richtig umgehen können, konfrontiert und jeden Tag tauchen neue Cyberbedrohungen auf, die unterschiedlich raffiniert sind. Die destruktivsten unter ihnen haben ganze IT-Systeme zum Absturz gebracht, medizinische Patientenakten beschädigt und den Betrieb eines ganzen Krankenhauses lahmgelegt.

Der als WannaCry bekannte Ransomware-Stamm aus dem Jahr 2017 führte zu einem Schaden von mehr als 4 Milliarden Dollar[1] und Klinikpersonal war gezwungen, klinische Daten mit Bleistift und Papier aufzuzeichnen und eine medizinische Versorgung ohne Zugriff auf die Patientenakten vorzunehmen.

Erkenntnis 2: Beziehungen und Zusammenarbeit sind der Schlüssel
Am Ende jeder Diskussion über Cybersicherheit im Gesundheitswesen und den Schutz medizinischer Daten steht letztlich ein einziges Wort: Vertrauen. In einem Ökosystem, das sich aus mehreren Interessengruppen zusammensetzt – Regulierungsbehörden, Führungskräfte im Gesundheitswesen, Ärzte, Patienten und Hersteller von Gesundheitstechnologie wie Philips Healthcare – spielt jede Partei eine wichtige Rolle.

Ein Bereich, in dem sich die Branche einig ist, ist die Notwendigkeit einer kontinuierlichen Koordination zwischen Leistungserbringern und Herstellern, um Sicherheitsbelange zu behandeln. Bei den Leistungserbringern werden Schritte unternommen, die Cybersicherheit von vornherein in die Technologie- und Netzwerkarchitektur zu integrieren, die Investitionen in Cybersicherheitsteams zu erhöhen und die Wertschöpfungskette im Bereich Sicherheit breiter zu betrachten.[2]

Durch die Zusammenarbeit im gesamten Ökosystem des Gesundheitswesens kann die Branche auf die Fortschritte anderer kritischer Infrastrukturbranchen aufbauen. Das unterstützt die Vorteile, die die digitale Konnektivität für die Patientenversorgung mit sich bringen wird. „Es gibt nicht die eine goldene Lösung. Statt es als Last zu sehen, müssen wir Sicherheit und Datenschutz in unsere Organisationen integrieren", sagt Dirk de Wit, Head of Global Product & Security Services, Philips. „Jeder von uns in diesem Ökosystem muss seine Rolle bei der Abwehr dieser Bedrohung spielen."

[1] More Disruption feared from Cyberattack, Reuters, 2017
[2] The Cyber-resilient enterprise, Accenture, 2018

Erkenntnis 3: Wissen aneignen und die richtigen Fragen stellen

In dem Beitrag „The Cyber-resilient enterprise" von Accenture heißt es, dass Führungskräfte „ihr Engagement für die Cybersicherheit verstärken – bis zu einem Punkt, an dem sie die Verantwortung für die Cyberrisiken des Unternehmens übernehmen.

Aber da Sicherheitsprogramme im Durchschnitt nur 67 Prozent des Unternehmens abdecken, haben die meisten noch viel mehr zu tun." Accenture empfiehlt allen leitenden Führungskräften, sich die folgenden Fragen zu stellen, um das volle Engagement für die Cybersecurity-Bedrohung zu ermitteln:

1. Hat der CIO/CISO die Aufsicht über mehr als nur die Unternehmenszentrale – über Abteilungen, Funktionen, Tochtergesellschaften, Joint Ventures? Anders ausgedrückt: Über welche Bereiche des Unternehmens hat der CIO/CISO keine Aufsicht?

2. Haben Sie bei neuen Geschäftsinitiativen, die das Cyber-Risiko erhöhen, den CIO/CISO in die Diskussionen einbezogen, um zu beraten, zu coachen und das Risiko zu thematisieren?

3. Haben Sie bei den Erwägungen zur Einführung neuer Technologien den CIO/CISO konsultiert, um Lösungen für Sicherheitsbedenken zu identifizieren und zu entwickeln?

4. Haben Sie bei Gesprächen mit dem CIO/CISO das Gefühl, dass Sie die gleiche Sprache sprechen?

5. Versteht der CIO/CISO, wohin Sie das Unternehmen führen wollen?

6. Wie sehen die Gespräche zwischen dem CIO/CISO und den Verantwortlichen im Unternehmen aus – konzentrieren sie sich auf technische und Compliance-Fragen oder auf die Auswirkung der Risiken auf den Geschäftserfolg?

Laut Accenture muss sich der CIO/CISO mit dem COO zusammenschließen, um ein Berater der Unternehmensführung zu werden. Gemeinsam können sie die Verantwortlichen im Unternehmen darauf vorbereiten, anders über Sicherheit zu denken, denn Sie geben den Ton für das gesamte Unternehmen an.

Erkenntnis 4: Planen Sie für den schlimmsten Fall

Organisationen des Gesundheitswesens sind wertvolle und sensible Infrastrukturen, aber sie müssen sich mit ständig wachsenden und immer raffinierteren Cyberbedrohungen auseinandersetzen. Es ist eine große Herausforderung für diese Organisationen, eine gute Cybersicherheit aufrechtzuerhalten, da viele Einrichtungen über sehr komplexe, vielschichtige Netzwerke mit einer fragmentierten Gesundheits-IT verfügen.

Die Daten im Gesundheitswesen sind zudem extrem wertvoll. Gesundheitsdaten enthalten sensibelste Daten an einem einzigen Ort, was sie sehr attraktiv für Identitätsdiebstahl, Abrechnungs- und Versicherungsbetrug sowie Erpressung macht. Im Gegensatz zu Kreditkartendaten, die Sie ändern und ersetzen können, können Sie Ihre Gesundheitsdaten nicht einfach ändern.

Vorbereitung ist der Schlüssel. In ihrer Umfrage zu Cybersicherheitsverletzungen aus dem Jahr 2019 berichtete die britische Regierung, dass rund die Hälfte (46 %) der britischen Unternehmen berichtet hat, dass sie 2019 einen Cyberangriff oder eine Datenverletzung erlebt haben – ein Anstieg von 39 % gegenüber dem Jahr 2018. Vor diesem Hintergrund sprechen die Cybersecurity-Experten von Philips die folgenden Empfehlungen aus, um Datenschutzverletzungen im Gesundheitswesen vorzubeugen und die Datensicherheit zu verbessern.

Fünf Tipps zur Prävention von Datenschutzverletzungen und für eine bessere Datensicherheit im Gesundheitswesen

1. Verschaffen Sie sich einen klaren Überblick
Erfassen Sie genau, welche Produkte und Anlagen sich in Ihrer Umgebung befinden.

2. Konzentrieren Sie sich auf ältere Produkte
Arbeiten Sie mit Technologiepartnern an allen älteren Produkten und Lösungen, die möglicherweise nicht aktualisiert, gepatched und gesichert werden können.

3. Entwickeln Sie Best Practices
Stellen Sie sicher, dass Sie ein Verständnis dafür haben, was aus Sicht der Branche Best Practices sind.

4. Steuern Sie die Cybersicherheit über die gesamte Lieferkette hinweg
Es ist wichtig, an Ihren Beschaffungsprozessen zu arbeiten und die Komponenten der von Ihnen bereitgestellten Lösungen zu verstehen.

5. Schließen Sie Partnerschaft mit Herstellern, Anbietern
Erwägen Sie, Ihre Hauptlieferanten (z. B. im Bereich der Bildgebungsinformatik) in die Steuerung und Reduzierung Ihrer Sicherheitsrisiken durch Sicherheitsstandards einzubeziehen, und nutzen Sie die Erfahrung und die Kapazitäten der Hersteller von Medizinprodukten, um Gesundheitsorganisationen bei der Erfüllung ihrer Pflichten in Bezug auf Cybersicherheit und Datenschutz, z. B. ITSiG und DS-GVO, zu unterstützen.

Erkenntnis 5: Sprechen Sie mit Philips über unsere branchenführenden Cybersicherheitslösungen

Bei Philips ist Security By Design eine durchgängige Denkweise: Die Einbindung von Sicherheitsprinzipien beginnt mit dem Produktdesign und der Entwicklung, über das Testen und die Bereitstellung – gefolgt von umfassenden Richtlinien und Verfahren für die Überwachung, effiziente Updates und, falls erforderlich, das Vorfallmanagement. Unsere Produkte lösen viele Kundenherausforderungen, aber Sicherheit ist immer inhärent in allem, was wir schaffen und vernetzen. Als erstes Unternehmen der Medizintechnikbranche hat Philips ein Security Center of Excellence (SCoE) eingerichtet, um Produkte zu entwickeln, die cyberresilient sind.

Mit dieser Denkweise, und als führendes Unternehmen im Bereich Gesundheitstechnologie und Hersteller von Medizinprodukten, bietet Philips Kunden eine umfassende Palette an Cybersicherheitsdiensten für den medizinischen Bereich, um sie bei der Bewältigung ihrer Cybersicherheitsrisiken bei vernetzten Medizingeräten und dem Schutz ihrer kritischen Ressourcen zu unterstützen. Unsere Lösungen wurden im Einklang mit globalen Best Practices für Cybersicherheit entwickelt und basieren auf dem NIST-Cybersicherheits-Framework (US National Institute of Standards and Technology). Sie decken so das gesamte Spektrum von Identifizierung, Schutz, Erkennung, Reaktion und Wiederherstellung ab.

Da der privilegierte Zugriff, der für Fernwartungsdienste erforderlich ist, ein erhebliches Risiko für Leistungserbringer darstellen kann, bietet Philips außerdem eine hochauflösende Überprüfung des Fernzugriffs und eine mögliche Integration mit führenden Lösungen für das Fernwartungszugriffsmanagement an. Und da viele Leistungserbringer wirtschaftliche Gründe haben, Altsysteme weiter zu nutzen, helfen die sicheren Lebenszyklus-verlängernden Services von Philips den Kunden, die Nutzungsdauer ihrer Medizinprodukte zu maximieren, indem sie Upgrade-Pfade und entschärfende Kontrollen zur Aufrechterhaltung akzeptabler Sicherheitsbedingungen bereitstellen.

Durch die integrierte Betrachtung von Mensch, Prozess und Technologie helfen die Beratungsdienstleistungen von Philips den Kunden bei der Einhaltung gesetzlicher Vorschriften sowie bei der Risiko- und Schwachstellenbewertung von medizinischen Systemen. Wir implementieren Sicherheitsstandards, welche die aktuellen gesetzlichen Vorschriften und die Best Practices der Branche erfüllen oder übertreffen, darunter:

- Die Risikoanalysen zur Produktsicherheit von Philips sind mit dem von der FDA empfohlenen Standard ISO/IEC-80001 und zahlreichen anderen Standards wie NIST 800- 53 Rev 4, ITIL v3.1.24 und den Standards der ISO/IEC-27000-Serie abgestimmt.

- Philips ist sowohl konform mit der ISO 14971, der EU-Richtlinie 95/46/EC als auch den HIPAA-Sicherheits- und Datenschutzbestimmungen.

- Erstellung von kundenorientierten Informationen, wie z. B. das branchenübliche „Manufacturer Disclosure Statement for Medical Device Security“ (MDS2).

- Unterstützung beim FDA-Leitfaden zum Premarket Management der Cybersicherheit bei Medizinprodukten und dem FDA Postmarket Management der Cybersicherheit bei Medizinprodukten.

- Geschulte Philips Fachleute verfügen über beträchtliches Fachwissen in den Bereichen Cybersicherheit und Medizinprodukte.

Zertifizierungen wie ISO27001, SOC 2 und HIPAA helfen beim Aufbau einer Vorreiterrolle und Glaubwürdigkeit im Bereich Cybersicherheit für Medizinprodukte.

Und natürlich bietet die Philips Healthsuite Plattform auch die Grundlage und den Rahmen für Sicherheit und Datenschutz in der vernetzten Cloud. Innerhalb der vernetzten Philips Healthsuite Cloud bildet das Information Security Management System (ISMS) diesen Rahmen, der für Sicherheit und Datenschutz bei der Erstellung von Plattformprodukten und -services sowie die Prozesse zur Risikobewertung und zum Vorfallmanagement steuert.

Sicherheitsmaßnahmen sind auf verschiedenen Ebenen eingebettet – Anwendungssicherheit, Rechnersicherheit, Datensicherheit, Informationssicherheit, Netzwerksicherheit – sowie administrative und betriebliche Schutzmaßnahmen. Sicherheits- und Datenschutzmaßnahmen sind im Entwicklungsprozess von Beginn an vorgeschrieben, um einen effizienten Datenschutz über alle Plattformfunktionen hinweg zu gewährleisten.

Philips übernimmt auch eine führende Rolle bei der Zusammenarbeit mit Aufsichtsbehörden wie BfArM, FDA und anderen internationalen Regulierungsbehörden, Industriepartnern und Leistungserbringern, um Schwachstellen zu schließen und Schutzmaßnahmen zu implementieren. Das Unternehmen beteiligt sich aktiv an maßgeblichen Branchengruppen, die sich mit Sicherheit oder Datenschutz befassen, darunter ZVEI, bvitg, AdvaMed, MITA und vielen anderen weltweit, und engagiert sich ebenfalls für Best Practices zur Identifizierung, Behebung und Veröffentlichung potenzieller Schwachstellen. Die Cybersicherheitsbeauftragten von Philips haben im Rahmen von Arbeitsgruppen für Cybersicherheit eine führende Rolle bei der Schaffung globaler Standards übernommen, darunter die International Cybersecurity Guidance In Initiative des International Medical Device Regulation Forum (IMDRF).

Überblick über die Cybersicherheitsservices von Philips im medizinischen Bereich

Philips Beratungsleistungen

Das Cybersecurity Consulting von Philips unterstützt Kunden bei der Einhaltung gesetzlicher Vorschriften sowie bei der Risiko- und Schwachstellenbewertung medizinischer Systeme, einschließlich der Beratung bei der Implementierung organisatorischer Prozesse, die Vorfallreaktions- und Wiederherstellungsabläufe mühelos bei allen Lieferanten integrieren. Wir beraten und helfen bei der Entwicklung von Strategien und Frameworks für Kunden, führen Sicherheits-Workshops durch und stellen Cybersicherheitsberater anbieterübergreifend bereit, um die Schaffung vertrauenswürdiger IT-Umgebungen zu gewährleisten.

Philips Protection Services

Die Philips Protection Services helfen Kunden, ihre Systeme durch koordinierte Offenlegung von Schwachstellen, medizinisch validiertes Patching und Netzwerksegmentierung sicher zu halten.

Erkennungs-, Reaktions- und Wiederherstellungsservices

Die Erkennungs-, Reaktions- und Wiederherstellungsservices von Philips helfen Kunden, ihre medizinischen Anlagen zu identifizieren und die Sicherheitslage ihrer medizinischen Systeme rund um die Uhr zu überwachen und bei Bedarf Reaktions- und Wiederherstellungsworkflows auszulösen, oder ebenso bei der Wiederherstellung nach Cybersicherheitsvorfällen zu helfen.

Sichere Lebensdauerverlängernde Services von Philips

Die Philips Secure Lifetime Extension Services helfen Kunden, die Nutzungsdauer ihrer medizinischen Geräte zu maximieren, indem sie entsprechende Maßnahmen zur Aufrechterhaltung einer akzeptablen Sicherheitslage bereitstellen.

Managed Security Services

Die Managed Security Services von Philips ergänzen die Managed Technology Services, indem sie das gesamte Portfolio an Sicherheitsdiensten übernehmen.

Sie möchten mehr erfahren?

Lassen Sie uns reden. Oder besser: Lassen Sie uns zusammenarbeiten.

Wir würden Ihnen gerne helfen, Operative Intelligenz anzuwenden, um Ihre wichtigsten Herausforderungen in Bezug auf Mitarbeiter, Prozesse und Technologie zu lösen.

Mehr erfahren Sie unter **www.philips.de/cybersecurity-services**

So erreichen Sie uns
Besuchen Sie uns auf www.philips.com
healthcare@philips.com