PHILIPS

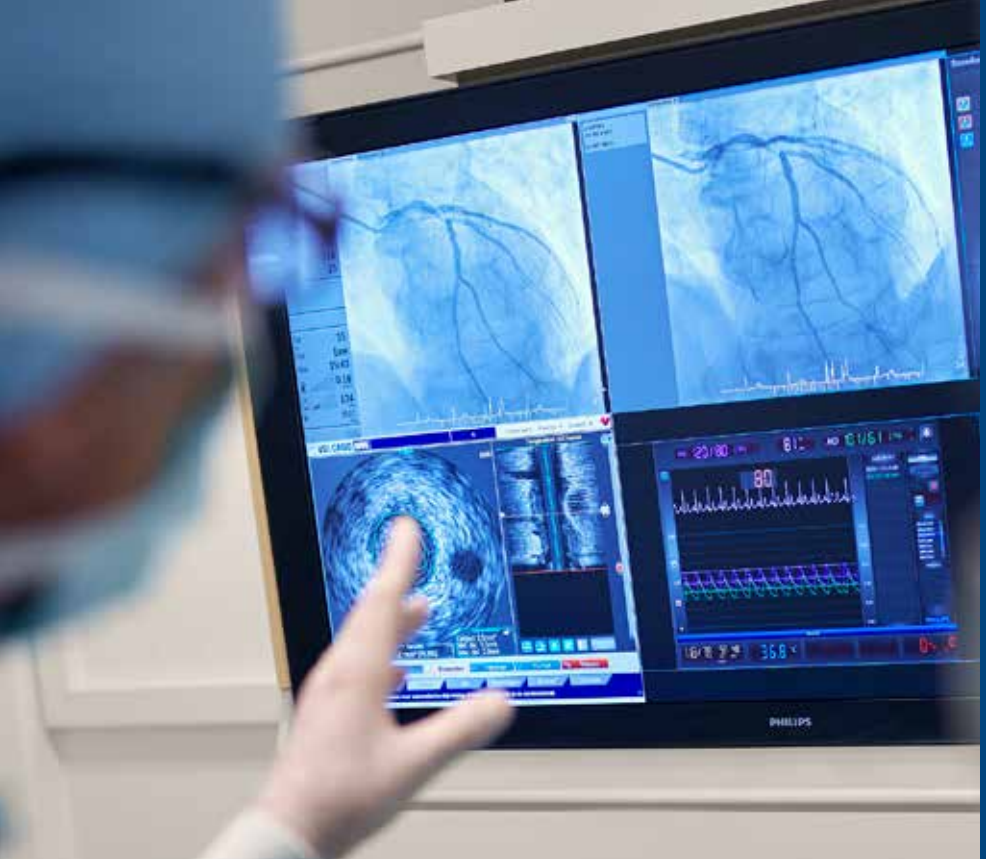
Positionspapier

Philips und Cybersicherheit

Die Sicherheit und der Datenschutz unserer Kunden stehen für uns an erster Stelle

Januar 2018

Inhalt



„Cybersicherheit ist das A und O beim Übergang zu einer vernetzten Versorgung.“

Jeroen Tas
Chief Innovation and Strategy Officer, Philips

1. Die Digitalisierung des Gesundheitswesens – Chancen und Gefahren

In Anbetracht der Herausforderungen einer alternden Bevölkerung stehen die Gesundheitssysteme heute vor dem Problem, geeignete und finanzierbare Versorgungsmodelle zu entwickeln. Ein vernetztes Gesundheitswesen – auf der Grundlage von vernetzten Geräten, Gesundheits-Apps und -Plattformen – besitzt beispielloses Potenzial zur Verbesserung der Versorgungsqualität bei vergleichsweise geringen Kosten.

Die Verfügbarkeit von Millionen von vernetzten digitalen Geräten ermöglicht Benutzern und Netzwerken den Austausch, die Suche, die Navigation, die Verwaltung, den Vergleich und die Analyse von bzw. in nahezu unbegrenzten Datenströmen, wodurch eine Verbesserung der Versorgungsergebnisse erzielt werden kann. Die digitale „Landschaft“ hat bereits dazu beigetragen, dass die Branche das Portfolio von persönlichen und gesundheitsorientierten intelligenten Geräten erweitert hat, was zu Innovationen und höherer Serviceeffizienz geführt hat.

Beispielsweise führt die Analyse von elektronischen Patientenakten und diagnostischen Informationen, die von Bildgebungsgeräten, Monitoren und persönlichen Mobilgeräten gesammelt werden, zu einer leichteren Entscheidungsfindung durch Ärzte und ermöglicht den Patienten eine aktivere Beteiligung an ihrer Gesundheitsversorgung.

Die exponentielle Zunahme der Menge und Arten der verfügbaren Daten führt jedoch auch zu einer größeren Anfälligkeit für Cyberkriminalität – Gesundheitsdaten sind das häufigste Angriffsziel für Cyberkriminelle und sind zehnmal wertvoller als Kreditkartendaten.

Personenbezogene Daten innerhalb von Patientenakten sind extrem wertvoll, da diese für zahlreiche kriminelle Zwecke verwendet werden können, beispielsweise zur Erstellung falscher Identitäten oder Geltendmachung unberechtigter Versicherungsansprüche.

Die Bedrohungen umfassen bösartige Angriffe über Viren oder Würmer und Eindringversuche durch Hacker. Bei den Tätern handelt es sich um Garagen-Hacker, Mitglieder der organisierten Kriminalität und sogar Nationalstaaten.

Cyberangriffe wie der Ransomware-Angriff WannaCry im Mai 2017 zeigen, dass selbst die größten und am besten geschützten Einrichtungen anfällig für Ausfälle sind. In diesem Fall mussten sogar einige Krankenhäuser ihre Patienten in andere Kliniken verlegen.

> 100.000.000
attackierte Datensätze in 2015

34% der betroffenen Datensätze stammen aus dem Gesundheitswesen.[1]

Über 75%
aller seriösen Websites enthalten **nicht behobene Schwachstellen.**[2]

Im Jahr 2016 wurden in den USA
zwei Milliarden
personenbezogene Datensätze gestohlen, darunter **100 Millionen** Patientenakten.[3]

Häufigstes Angriffsziel

Gesundheitswesen ist primäres Angriffsziel

Die Wiederherstellung einer verlorenen oder gestohlenen Patientenakte könnte bis zu **363 USD pro Akte** kosten.[4]

Die durch
Cyberkriminalität
verursachten Kosten erreichen bis 2019 voraussichtlich **2 Billionen USD**.[5]

Die der Weltwirtschaft durch Cyberkriminalität verursachten Kosten betrugen im Jahr 2016 über
450 Milliarden USD.[6]

Quellen:

1. IBM X-Force Threat Intelligence Report 2016
2. Symantec
3. CNBC
4. IBM X-Force Threat Intelligence Report 2016
5. Juniper Research
6. CNBC

2. Philips' Position zur Cybersicherheit

Philips liefert Innovationen, die Endabnehmern und medizinischem Fachpersonal eine einfachere Vernetzung und fundiertere Entscheidungen ermöglichen. Einige der leistungsfähigsten und vielversprechendsten Chancen für Innovationen im Gesundheitswesen beruhen auf Forschungen mit großen Studiengruppen und großen Datenmengen.

Die strategische und kompetitive Position von Philips basieren im hohen Maße auf **Daten, digitaler Innovation und dem Vertrauen der Kunden**.

Philips verarbeitet ständig wachsende Mengen von gesundheitsbezogenen Daten, den sensibelsten personenbezogenen Daten überhaupt. **Unsere Kunden verlangen ein hohes Maß an Sicherheit in Bezug auf unsere Sicherheits- und Datenschutzmaßnahmen**. Unsere Maßnahmen zum Datenschutz nehmen eine immer entscheidendere Rolle bei den Geschäftsabschlüssen mit Partnern ein.

In Anbetracht der Sorgen unserer Kunden und der Endabnehmer und der wichtigen Rolle, die die Sicherheit in der heutigen vernetzten digitalen Landschaft spielt, entwickelt Philips **umfassende Sicherheitspläne**, um die Sicherheit von Produkten, Unternehmen (Unternehmensdaten) und personenbezogenen Patientendaten zu gewährleisten.

Unsere Sicherheitspläne beziehen sich auf unsere **Mitarbeiter, Prozesse und Technologien**, mit dem Ziel, die **Vertraulichkeit, Integrität und Verfügbarkeit** wichtiger Daten und der sie enthaltenden Systeme sicherzustellen.

Das Konzept von **Security by Design** von Anfang bis Ende – von der Entwicklung, über die Fertigung bis zum Kundendienst – ist für den langfristigen Erfolg unserer Produkte, Dienstleistungen und Lösungen von größter Wichtigkeit.

Philips fördert proaktiv die kontinuierliche Umsetzung von Strategien zur Verringerung von Risiken und Bedrohungen, einschließlich der wesentlichsten Sicherheitsrisiken:

- **Kennwortrisiko**: das Risiko aufgrund des Fehlens einer sicheren Verwaltung von Identitäten und Berechtigungen, z.B. Multifaktor-Authentifizierung
- **Verschlüsselungsrisiko**: das Risiko aufgrund des Fehlens einer Datenverschlüsselung von Anfang bis Ende – von der Erstellungsquelle der Daten, über das Netzwerk, bis zum Ruhezustand im Rechenzentrum – und/oder einer effektiven Lösung zur Verhinderung von Datenverlust
- **Risiko des Patch-Managements**: das Risiko des Fehlens eines effektiven Patch-Managements, durch das beispielsweise Schwachstellen in älteren Betriebssystemen entstehen

Sicherheit ist – wie Zuverlässigkeit und Qualität – eine Voraussetzung für das Vertrauen in die Marke Philips. **Kunden und Endabnehmer müssen sich auf die Sicherheit, Zuverlässigkeit und Qualität unserer Produkte und Dienstleistungen verlassen können** und einen Vorteil in der Weitergabe ihrer Daten erkennen – andernfalls lassen sich die aus Konnektivität und der Analyse von „Big Data" ergebenden gesundheitlichen Vorteile möglicherweise niemals erzielen. Daher betonen wir immer wieder die Vorteile vernetzter Gesundheitstechnologie und investieren weiterhin in sichere Systeme, auf die sich Kunden verlassen können.

"Produkt- und Informationssicherheit ergeben sich aus einer Kombination aus Aufklärung, Richtlinien und Verfahren sowie physischer Sicherheit und Technologie."

Michael McNeil
Head of Global Product and Security Services, Philips

3. Transparenz, Konformität und mehr

Philips implementiert Sicherheitsmaßnahmen innerhalb einer stark regulierten Medizinproduktbranche. Aufsichtsbehörden wie die US-amerikanische Food and Drug Administration verlangen, dass auf den Markt gebrachte Hardware und Software und etwaige Änderungen einer strengen Verifizierung und Validierung unterzogen werden müssen, damit die **hohen Sicherheits-, Zuverlässigkeits-, Effizienz-, Qualitäts- und Leistungsstandards** bei allen Produkten und Dienstleistungen von Philips eingehalten werden können.

Philips garantiert die **Konformität** mit Normen und Richtlinien zu Datensicherheit und Datenschutz.

Philips ist bestrebt, **beim Melden und Beheben von Schwachstellen einen offenen und transparenten** Ansatz zu verfolgen und hat einen robusten Prozess zur „Koordinierten Offenlegung von Schwachstellen“ (Coordinated Vulnerability Disclosure) entwickelt (bisher als „Verantwortungsbewusste Offenlegung“ (Responsible Disclosure) bezeichnet).

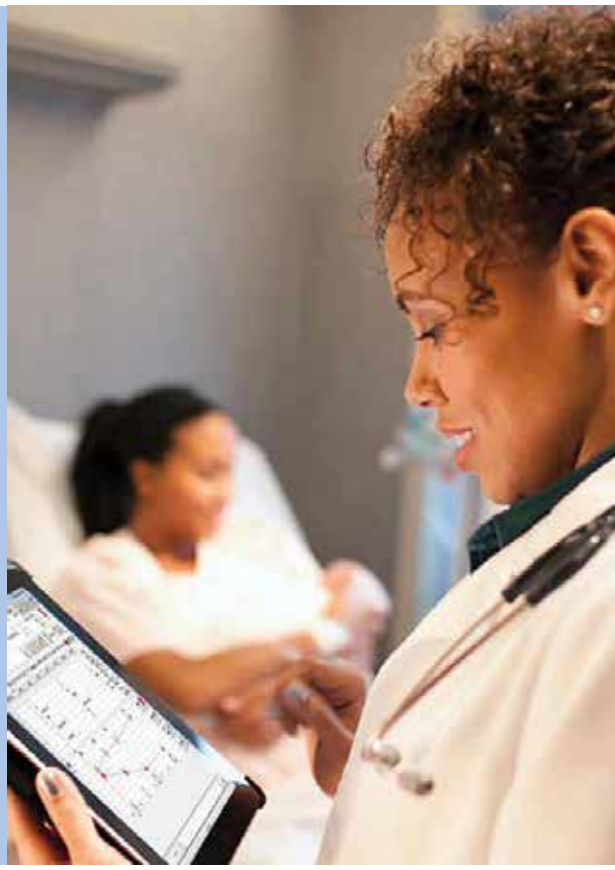
Zu unserer Strategie gehört nicht nur, stets über aufkommende Sicherheitsschwachstellen und potenzielle externe Bedrohungen informiert zu sein, sondern auch die **Übernahme von Verantwortung und die Zusammenarbeit** mit Aufsichtsbehörden, Branchenpartnern, Gesundheitsdienstleistern und anderen, um Sicherheitslücken zu schließen und Sicherheitsmaßnahmen zu implementieren.

Zur weiteren Bündelung unserer Anstrengungen **beteiligt sich Philips aktiv an wichtigen Branchengruppen**, die ihren Fokus auf Sicherheit und Datenschutz richten. Wir möchten sicherstellen, dass adäquate und erforderliche Anforderungen an die Kundensicherheit in Branchenstandards, Richtlinien und Initiativen Eingang finden.

Philips unterstützt die „Empfehlungen für öffentlich-private Partnerschaften gegen Cyberkriminalität“ des **Weltwirtschaftsforums**.

„Patientensicherheit in den vernetzten Versorgungsumgebungen von heute ist eine Aufgabe, die wir alle sehr ernst nehmen. Während wir alle unsere Programme zur Cybersicherheit weiterentwickeln, müssen Transparenz, Verantwortungsbewusstsein und Reaktionsbereitschaft Prioritäten darstellen, die weiterhin zu fördern sind.“

Michael McNeil
Head of Global Product and Security Services, Philips



4. Produktsicherheit

Philips nimmt die zunehmenden Risiken für unsere Produkte durch Bedrohungen der Cybersicherheit[1] sehr ernst. Wir haben seit Langem Anstrengungen unternommen, unsere Prozesse und Systeme kontinuierlich zu verbessern, um die Risiken für die Patienten, die von unseren Lösungen und Dienstleistungen abhängig sind, zu minimieren.

Uns ist der zunehmende Trend zu hoch entwickelten Cyberangriffen in zahlreichen Branchen – und in zunehmendem Maße im Gesundheitswesen – vollkommen bewusst. In dem Maße wie Krankenhausnetzwerke, klinische Datenbanken, medizinische Geräte und persönliche Gesundheits-Überwachungssysteme immer mehr integriert werden, wächst auch das Potenzial für Cybersicherheits-Schwachstellen.

Philips hat als einer der ersten erkannt, dass es bei effektiver Cybersicherheit nicht mehr darum geht, die „Packung" bzw. das einzelne Produkt zu schützen, sondern ein systematisches Konzept zu entwickeln, das in Betracht zieht, wo und wie ein Gerät genutzt wird. **Bei Philips ist „Security Designed in" ein ganzheitliches Konzept: Die Umsetzung von Sicherheitsprinzipien beginnt mit der Produktkonzeption und -entwicklung und setzt sich über die Tests und Bereitstellung fort – und wird mit robusten Richtlinien und Verfahren zur Überwachung, effektiven Aktualisierungen und, falls erforderlich, einem Reaktionsmanagement bei Vorfällen nachverfolgt.**

Damit unsere Produkte und Dienstleistungen widerstandsfähig gegen Cyberbedrohungen sind, sind permanente Risikobewertungen und eine sicherheitsbewusste Produktentwicklung erforderlich. Weiterhin sind eine schnelle Bereitstellung sicherheitsunterstützender Technologien wie Verschlüsselung und Patch-Management sowie kontinuierliche Verbesserungen unverzichtbar. Aus diesem Grund haben wir unser „Sicherheitsprogramm für Produkte und Lösungen" gestartet, um umfassende und effektive Konzepte zur Erfüllung der Anforderungen unserer Kunden zu entwickeln, zu implementieren und zu aktualisieren.

Wichtige Initiativen von Philips zur Produktsicherheit sind:
Veröffentlichung einer branchenführenden, öffentlich verfügbaren „Philips Produktsicherheitsrichtlinie", bestehend aus Richtlinien, Verfahren und Standards, die es dem Unternehmen ermöglichen, optimale Verfahren zur Sicherheit zu implementieren.

Die Richtlinie definiert unsere strategische Organisation und die Verfahren für:

- Beschäftigung eines globalen Netzwerks von Sicherheits- und Datenschutzexperten, die entsprechend der Philips Produktsicherheitsrichtlinie arbeiten
- Entwicklung und Bereitstellung von optimalen Verfahren für unsere Produkte und Dienstleistungen
- Durchführung von Risikobewertungen und Ergreifung von Reaktionsmaßnahmen bei Vorfällen in Bezug auf potenzielle und festgestellte Sicherheits- und Datenschutzbedrohungen und -schwachstellen
- Einbindung und Aktualisierung von Sicherheitskomponenten in Produkte und Dienstleistungen während des gesamt Lebenszyklus, einschließlich Risikobewertung und Reaktion auf erkannte Schwachstellen

Implementierung von Sicherheitsstandards, die gegenwärtige gesetzliche Anforderungen und bewährte Verfahren der Branche erfüllen oder übertreffen, z.B.:

- Produktsicherheit und Datenschutzanforderungen für Produkte und Dienstleistungen, die nicht nur der von der FDA empfohlenen Norm ISO/IEC-800001 entsprechen, sondern die Grundlage für die Norm 80001-2-2 darstellten
- Dienstleistungssicherheit und Datenschutzanforderungen entsprechend anerkannten Normen wie NIST 800-53 Rev 4, ITIL v3.1.24 und der ISO/IEC-27000-Reihe
- Bereitstellung von Informationsmaterial wie „Manufacturer Disclosure Statement for Medical Device Security" (MDS[2])
- Unterstützung bei den FDA-Anleitungen „Premarket Management on Cybersecurity in Medical Devices" und „Postmarket Management of Cybersecurity in Medical Devices".

Das Philips Security Center of Excellence tauscht Informationen mit führenden Forschungs- und Testeinrichtungen zur Cybersicherheit auf der ganzen Welt aus und unterstützt diese bei der schnellen Beseitigung, Verringerung und Behebung von Cyberbedrohungen.

Überwachung von Bedrohungen und Schwachstellen sowie Reaktion auf Sicherheitsvorfälle:

- Philips überwacht kontinuierlich auf neue Sicherheitsbedrohungen, Schwachstellen und Sicherheitsvorfälle, einschließlich Schwachstellen in Betriebssystemen sowie solcher, die von Anbietern von Drittanbieter-Software, Kunden und Sicherheitsforschern ermittelt werden.
- Die Philips Product Security Incident Response Teams bewerten potenzielle Sicherheitsvorkommnisse und festgestellte Schwachstellen und entwickeln geeignete Reaktionspläne.

Malware-Schutz und Patch-Management:

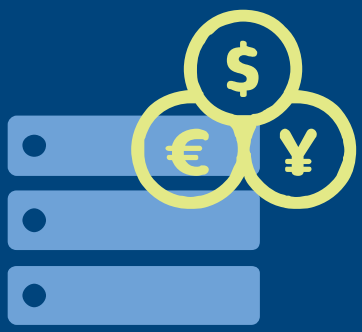
- Produkte werden entweder mit vorinstallierter Anti-Viren-Software geliefert oder enthalten eine entsprechende Kundendokumentation. Diese beschreibt die produktspezifischen Parameter für die von Philips freigegebene Anti-Viren-Software.
- In Philips Produkten wird möglicherweise Drittanbieter-Software verwendet, beispielsweise Betriebssysteme wie Microsoft Windows und Linux. Die Beurteilung der Auswirkungen dieser Hotfixes durch die Philips Produktentwicklungsteams beginnt in der Regel innerhalb von 48 Stunden, nachdem Philips Kenntnis von einer neuen Sicherheitslücke oder von der Verfügbarkeit eines Patches erhalten hat.

Eine Richtlinie zur verantwortungsbewussten Offenlegung bei der Meldung und Behebung von festgestellten Schwachstellen:

- Wir haben zu diesem Zweck eine Richtlinie für „verantwortungsbewusste Offenlegung“ eingeführt, die von der Branche als bewährtes Verfahren anerkannt wurde.
- Unsere Richtlinie für verantwortungsbewusste Offenlegung ist öffentlich zugänglich und enthält eindeutige Kommunikationskanäle für Kunden, Forscher und andere Interessenvertreter der Sicherheitsgemeinschaft.
- Die Richtlinie beinhaltet die Überwachung von eingehender Kommunikation und deren Beantwortung, Nachverfolgung, Bewertung von gemeldeten Schwachstellen und Statusverfolgung sowie Anwendung der entsprechenden Richtlinien zur Reaktion, Behebung und Verhinderung von Vorfällen.

Philips wird weiterhin strategische und effektive Maßnahmen entwickeln, um die Sicherheit von Medizinprodukten zu verbessern. Wir freuen uns darauf, diese wichtige Diskussion fortzusetzen, um unser Ziel zu erreichen, die Lebensqualität von Milliarden von Menschen zu verbessern.

1. Cybersicherheit beinhaltet alle Technologien, Prozesse und Praktiken zum Schutz von Netzwerken, Computern, Programmen und Daten vor Angriffen, Schäden und unberechtigtem Zugriff: http://whatis.techtarget.com/definition/cybersecurity



„Daten sind die neue Währung und Hacking ist ein Geschäftsmodell. Die Gewinne durch Hacking werden bald diejenigen des weltweiten Drogenhandels übertreffen.“

Stef Hoffman
Chief Information Security Officer, Philips

5. Informationssicherheit im Unternehmen

Das Wachstum von Philips basiert auf innovativer Technologie, der unsere Kunden vertrauen und auf die sie sich verlassen. Das Design, die Entwicklung und Fertigung dieser Technologie wird durch hoch entwickelte interne Informationssysteme ermöglicht.

In Anbetracht der wachsenden Bedrohung der Cybersicherheit, die sich gegen Technologien und die darin gespeicherten Daten richtet, verfolgt die Organisation Philips Information Security das Ziel, Informationssysteme des Unternehmens zu schützen und Folgendes sicherzustellen:

- **Vertrauen unserer Kunden:** Weiterentwicklung der Marke Philips zu einem Synonym für Zuverlässigkeit, Qualität und Sicherheit
- **Fähigkeit und Knowhow:** Verhindern des Verlusts von firmeneigenen Informationen, um die langfristige Wettbewerbsfähigkeit des Unternehmens zu sichern
- **Leistungsfähigkeit:** Schutz von Unternehmensressourcen zur Verhinderung negativer finanzieller Auswirkungen wie Verlust von Kunden, Umsatz und Gewinn
- **Betriebliche Stabilität:** Aufrechterhaltung des kontinuierlichen Betriebs durch die Verhinderung einer Beeinträchtigung oder Unterbrechung wichtiger Infrastruktur
- **Konformität mit Bestimmungen:** Sicherstellung, dass die Informationssysteme alle gesetzlichen Anforderungen erfüllen oder übertreffen

Informationssicherheit kann nicht durch Technologie alleine erreicht werden. Eine umfassende Informationssicherheit erfordert die Einbeziehung der drei Faktoren Mitarbeiter, Prozesse und Technologien (siehe nächste Seite). Die Organisation Philips Information Security implementiert Kontrollmechanismen für diese drei Faktoren, um Folgendes sicherzustellen:

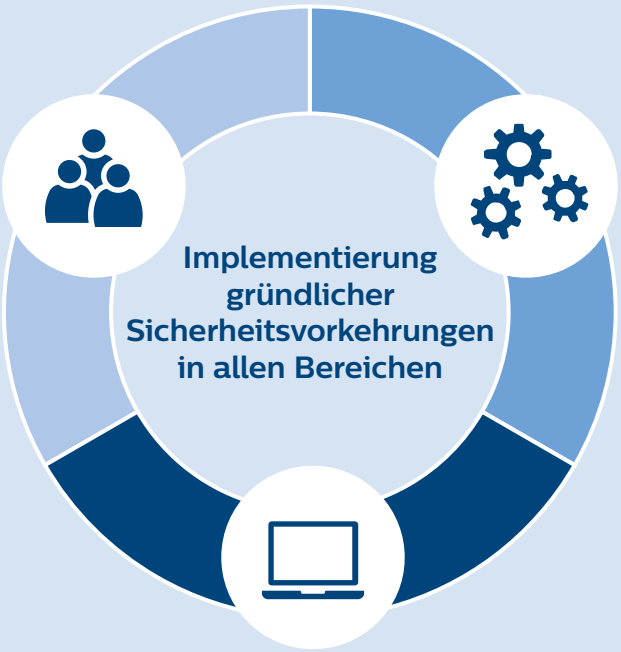
- **Vertraulichkeit:** Das Abrufen von Daten ist auf diejenigen beschränkt, die Zugang haben dürfen.
- **Integrität:** Informationen können nicht unbemerkt verändert werden.
- **Verfügbarkeit:** Auf Informationen kann zugegriffen werden, wenn Sie benötigt werden.

Philip stellt sich zum Schutz von Informationssystemen des Unternehmens und zur Stärkung des Kundenvertrauens den Herausforderungen einer zunehmenden Bedrohungslandschaft – und wird dies auch weiterhin tun. Die Organisation Philips Information Security wird auch weiterhin in die Bindung hervorragender Mitarbeiter für Cybersicherheit investieren und bewährte Verfahren zur Sicherheit in alle unsere Handlungen integrieren.

Datenschutz – Konzentration auf Mitarbeiter, Prozesse und Technologie

Mitarbeiter

Konzentration auf das Verhalten von Mitarbeitern mit dem Ziel, ihr Sicherheitsbewusstsein zu verbessern, was zur Entwicklung einer Sicherheitskultur führt

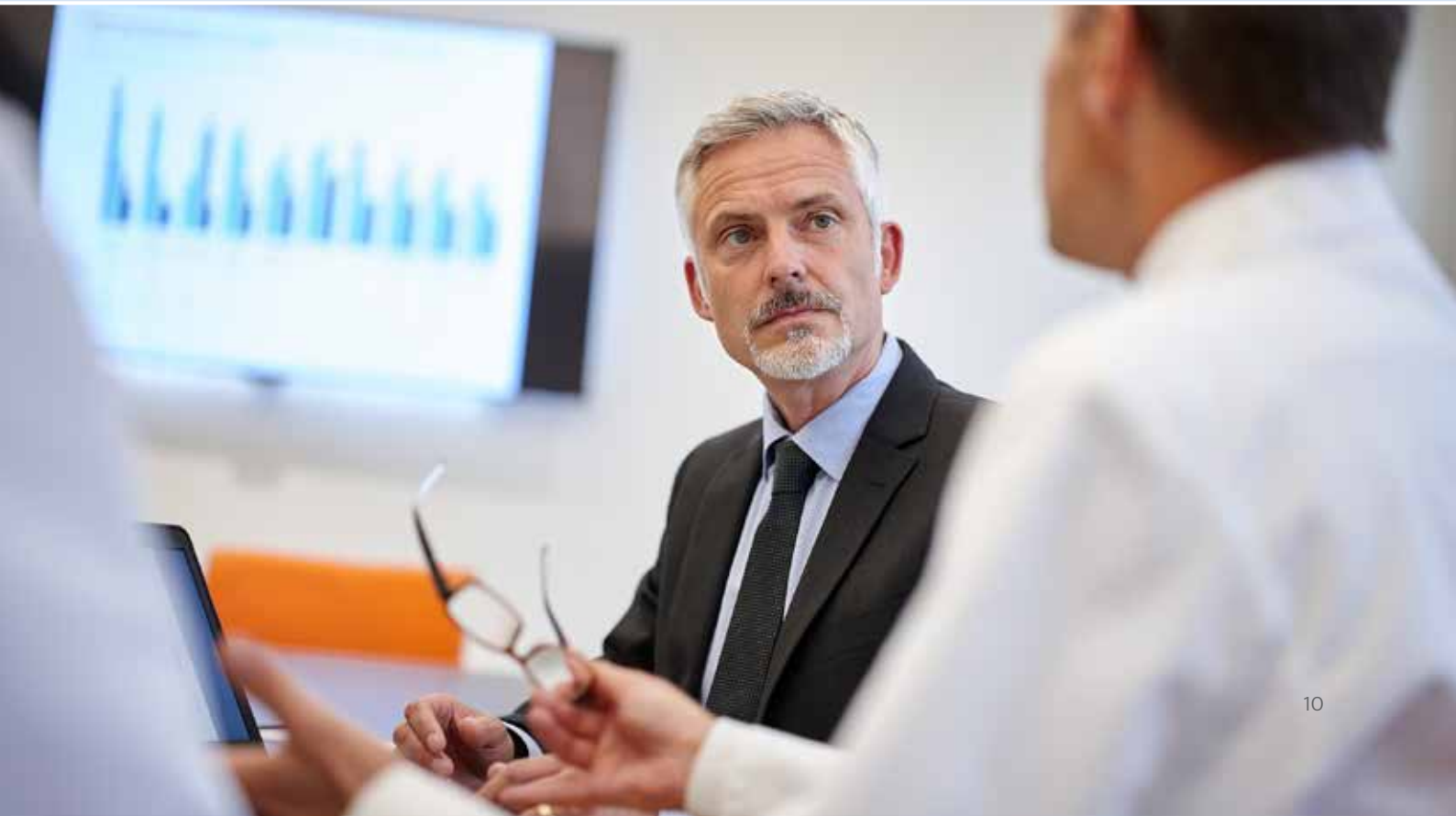


Prozesse

Konzentration auf unsere Geschäftsprozesse und Sicherstellung, dass Sicherheitsrisiken bewertet und adäquate Schritte zur Verringerung dieser Risiken implementiert werden

Technologie

Konzentration auf das Verstehen und die Überwachung unserer Technologielandschaft und Umsetzung technologischer Verbesserungen zu Verringerung unseres Sicherheitsrisikos



6. Datenschutz

Die Wahrung der Vertraulichkeit der Daten unserer Kunden, Endabnehmer und anderer Menschen, mit denen wir zu tun haben, wie Patienten, ist seit Langem ein Handlungsgrundsatz von Philips. Durch Transparenz beim Umgang mit personenbezogenen Daten entsteht Vertrauen. In dem Maße wie wir uns zu einem digitalen Unternehmen entwickeln ist die Einhaltung unserer Datenschutzstandards in zunehmendem Maße wichtig, um dieses Ziel zu erreichen.

In Anbetracht unseres Schwerpunktes auf Gesundheitstechnologie haben Datenschutz und -sicherheit eine strategisch wichtige Bedeutung erlangt, da Gesundheitsdaten zu den sensibelsten personenbezogenen Daten überhaupt gehören. Unsere Wettbewerbsposition ist in hohem Maße von diesen Daten abhängig, sodass öffentliches Vertrauen unverzichtbar ist. **Unsere Verpflichtung zum Datenschutz geht über die Einhaltung gesetzlicher Bestimmungen hinaus** und wir integrieren Kontrollmechanismen für Datenschutz und -sicherheit in den gesamten Lebenszyklus aller Daten.

Datenschutz und -sicherheit sind ein integraler Bestandteil unserer **allgemeinen Geschäftsprinzipien**, wobei für uns unter anderem folgende Verpflichtungen gelten:

- Die Implementierung von verbindlichen internen Datenschutzvorschriften, die eine Grundlage für den Datenschutz bei Philips weltweit darstellen und den internationalen Datenaustausch zwischen Unternehmen der Philips Unternehmensgruppe ermöglichen.
- Implementierung eines Datenschutzprogramms und einer Betriebsstruktur, durch die Datenschutz und -sicherheit im Unternehmen verankert werden
- Begrenzte Erfassung von Daten und wenn möglich, Einholung der Zustimmung der betroffenen Personen
- Benachrichtigung der betroffenen Personen, wie die erfassten Daten verwendet werden und Zusicherung der Ausübung der persönlichen Rechte
- Ergreifen der geeigneten Maßnahmen zur Erhaltung der Genauigkeit und Relevanz der Daten
- Schutz der personenbezogenen Daten unter Verwendung geeigneter Sicherheitsstandards

Als weltweit tätiges Unternehmen muss Philips alle nationalen Gesetze zu Datenschutz und -sicherheit beachten. Unsere verbindlichen internen Datenschutzvorschriften und unser Datenschutzprogramm verfolgen das Ziel von weltweiter Datenschutzkonformität bei Philips, selbst, wenn keine Datenschutzgesetze existieren.

Philips ist durch die Prinzipien **„Privacy by Design“** hohen Sicherheitsstandards und einer verantwortungsbewussten Datenverwaltung verpflichtet. Ziel dieses Konzepts ist die Integration von Kontrollmechanismen für Datenschutz und -sicherheit innerhalb des gesamten Datenlebenszyklus, von den ersten Entwicklungsstufen, über die Bereitstellung, Erfassung, Verwendung und schließlich die Vernichtung der Daten.

Damit die durch „Big Data“ möglichen Fortschritte im Gesundheitswesen erzielt werden können, müssen wir das Vertrauen der Menschen pflegen und ihnen den Wert erklären. Wir müssen das grundsätzliche Recht auf Datenschutz sicherstellen, und dank unserer Verpflichtung zu hohen Sicherheitsstandards und verantwortungsvoller Datenverwaltung können wir Ängste und Zweifel abbauen und Kunden durch kontinuierliche Innovation einen noch größeren Mehrwert bieten.

7. Vorhandene Strukturen und Mechanismen

- Die **verbindlichen internen Datenschutzvorschriften** sind interne Regeln für die Verarbeitung personenbezogener Daten bei Philips, die auch als Philips Datenschutzregeln (Philips Privacy Rules) bezeichnet werden. Die Philips Datenschutzregeln basieren im Wesentlichen auf den Datenschutzanforderungen der EU und den Datenschutzprinzipien der OECD. Sie stellen einen robusten Datenschutzrahmen für unser Unternehmen dar. Die Philips Datenschutzregeln legen allgemeine Datenschutzanforderungen fest, die für Philips weltweit gelten und den internationalen Austausch von personenbezogenen Daten innerhalb von Philips ermöglichen.

- **Lieferanten**, die im Namen von Philips Daten verarbeiten, müssen die striktesten Anforderungen erfüllen, wie sie in den verbindlichen internen Datenschutzvorschriften dargelegt sind.

- Wir unterhalten spezielle Centers of Excellence für Datenschutz, Produktsicherheit und Informationssicherheit. Das **Philips Global Privacy Office** unterstützt Philips Mitarbeiter bei der Erfüllung der Datenschutzanforderungen und legt den allgemeinen Rahmen für Datenschutzkonformität und Risikobewertung fest.

- Das **Philips Product Security & Services Office** ist für die Integration von Sicherheit in Produkte und Dienstleistungen während ihres gesamten Lebenszyklus verantwortlich. Dies beinhaltet Sicherheits-Risikobewertungen der Produkte, projektunabhängige Schwachstellen- und Penetrationstests, spezielle Schulungen zur Produktsicherheit sowie Reaktionen auf Schwachstellen, die in vorhandenen Produkten und Dienstleistungen unter Support ermittelt werden.

- Wir verfolgen bei der Informationssicherheit ein ganzheitliches Konzept von Anfang bis Ende. Wir verfügen über Prozesse und Strukturen, um sicherzustellen, dass jeder Schritt des Produktentwicklungs-Lebenszyklus mit einem hohen Maß an Vertraulichkeit und Integrität erfolgt. Im Rahmen dieses **sicheren Produktentwicklungs-Lebenszyklus** überwachen wir kontinuierlich auf Schwachstellen und validieren Fehlerbehebungen; Aktivitäten, die von unserem internen Security Center of Excellence unterstützt werden.

- Wir unterhalten ein **Schulungsprogramm für alle Mitarbeiter**, das den Schutz personenbezogener Daten sowie die erforderlichen Maßnahmen zur Einhaltung der Datenschutzregeln von Philips und der geltenden Gesetze zum Gegenstand hat. Mitarbeiter, die mit der Verarbeitung sensibler Daten befasst sind, erhalten eine zusätzliche stellenabhängige Schulung, um eine ordnungsgemäße Datenhandhabung zu gewährleisten. Zudem verfügen wir über spezielle Sicherheitsschulungsprogramme für unsere Entwicklungsteams.

- Für unsere **digitalen HealthSuite Plattformen** beauftragen wir Tier-1-Drittanbieter mit dem Hosten einiger technischer Dienstleistungen (z.B. Amazon und salesforce.com). Diese Anbieter müssen sich jährlich von unabhängigen Auditoren gemäß ISO/IEC 27001 und gegebenenfalls bezogen auf andere relevante Sicherheits- und Datenschutznormen (wie HIPAA/HITECH, SSAE Nr. 16, NIST SP800-53) zertifizieren lassen.

8. Weitere Informationen

Informationen zu Philips Product Security ›

Webseite zur Philips Datenschutzrichtlinie ›

www.philips.de/healthcare