Stellungnahme zur Produktsicherheitsrichtlinie

Philips Healthcare

In diesem Dokument wird die Position von Philips Healthcare in Bezug auf die Sicherung unserer Medizinprodukte und -systeme in Ihrer Einrichtung zusammengefasst. Außerdem werden unsere Prozesse beschrieben, mit denen wir in Zukunft Produkte mit integrierter Sicherheit *(Security Designed In)* anbieten möchten.

Hintergrund

Philips Healthcare legt größten Wert darauf, Sie bei der Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit sowohl der elektronischen geschützten Gesundheitsdaten als auch der Hardware- und Software-Produkte, von denen diese Daten erstellt und verwaltet werde, zu unterstützen.

In den letzten Jahren war ein dramatischer Anstieg bei den Bedrohungen der Sicherheit von Geräten und Gesundheitsdaten zu verzeichnen. Solche Bedrohungen liegen u.a. in Form bösartiger Sicherheitsangriffe durch Viren, Würmer oder direkten Systemzugriff durch Hacker vor. Regierungen in aller Welt haben Gesetze verabschiedet, um viele dieser Angriffe zu einem Straftatbestand zu erklären und Gesundheitsdaten zu schützen, die Rückschlüsse auf die Person des Patienten erlauben (z.B. HIPAA in den USA, BC 73, allgemeine Datenschutzbestimmungen unter der Europäischen Direktive 95/46/EG, Japan HPB517 und andere).

Um seinen Verpflichtungen hinsichtlich der Sicherheit nachzukommen, betreibt Philips Healthcare ein globales Programm, mit dem (a) moderne Sicherheitsfunktionen für unsere Produkte und Dienstleistungen entwickelt und implementiert werden und (b) der Umgang mit Datensicherheitsereignissen in der Praxis geregelt wird. Auf der Ebene der Medizinproduktbranche beteiligt sich Philips an der Medical Device Security Workgroup der HIMSS[1] und setzt sich dafür ein, dass neue Kundensicherheitsoptionen wie etwa Integrated Healthcare Enterprise in die Industriestandards aufgenommen werden[2]. Wir arbeiten außerdem an einer kontinuierlichen Verbesserung unseres eigenen internen Sicherheitssystems Information Technology Enterprise und streben dabei kontinuierliche Sicherheitsverbesserungen in den Bereichen Produktentwicklung und Leistungserbringung an.

Philips Healthcare implementiert Sicherheitsmaßnahmen innerhalb einer stark regulierten Medizinproduktbranche. Behördliche Bestimmungen (z.B. der US-amerikanischen Food and Drug Administration) verlangen, dass Hardware- und Software-Änderungen einer strengen Verifizierung und Validierung unterzogen werden müssen, damit die hohen Sicherheits- und Leistungsstandards ausnahmslos bei allen medizinischen Geräten von Philips eingehalten werden können[3].

Produktsicherheitsmaßnahmen von Philips Healthcare

Organisation

Philips Healthcare verfolgt eine globale Produktsicherheitsrichtlinie, in der die Berücksichtigung der Datensicherheit bei der Produktkonzeption sowie die Risikobeurteilung und die Reaktion auf Vorfälle geregelt sind, bei denen Sicherheitslücken in bestehenden Produkten identifiziert werden. Der Director of Product Security beaufsichtigt die Implementierung dieser Richtlinie und berichtet direkt an den Philips Healthcare Chief Technology Officer. Philips Healthcare hat ein globales System zur Problemverfolgung und Eskalation aufgebaut, damit schnell auf Sicherheitsprobleme reagiert werden kann. Das Management ist dabei stets auf dem aktuellen Stand der Dinge.

Überwachung von und Reaktion auf Sicherheitslücken

Produktentwicklungsgruppen innerhalb von Philips Healthcare befassen sich fortwährend mit neuen Sicherheitslücken, einschließlich der Probleme, die von den Herstellern von Drittanbieter-Software und Betriebssystemen identifiziert oder von Ihren Gesundheitseinrichtungen gemeldet wurden. Ein globales Netzwerk aus Product Security Officers und deren Teams sammelt und verwaltet Informationen und arbeitet an der Behebung von Sicherheitslücken, die Produkte und Lösungen von Philips Healthcare betreffen.

PHILIPS

Die Philips Product Security Incident Response Teams bewerten jede reale oder potenzielle Sicherheitsverletzung anhand einer expliziten Bedrohungs-/Sicherheitslücken-/Risikobeurteilung und entwickeln bei Bedarf Reaktionspläne gegen Sicherheitslücken. Wir möchten Sie – unsere Kunden – über Sicherheitslücken informieren, die Auswirkungen auf Ihre Systeme haben, und umgehend mit der Entwicklung und Umsetzung einer Abhilfemaßnahme beginnen, während Sie weiterhin alle notwendigen Informationen erhalten.

Patch-Management bei Betriebssystemen

Einige Produkte von Philips Healthcare nutzen handelsübliche Software und/oder handelsübliche PC-Betriebssysteme anderer Hersteller, z.B. Microsoft Windows. Philips sondiert ständig die relevanten Sicherheitsmitteilungen, die von den Herstellern und der Branche/den Medien veröffentlicht werden, und führt Risikobeurteilungen an aktuellen Medizinprodukten durch, die am stärksten von den neu entdeckten Sicherheitslücken betroffen sind.

Microsoft veröffentlicht regelmäßig Informationen zu Security-Patches (Hotfixes) zu MS Windows. Die Beurteilung der Auswirkungen dieser Hotfixes durch die Philips-Produktentwicklungsteams beginnt in der Regel spätestens 48 Stunden, nachdem Philips Kenntnis von einer neuen Sicherheitslücke oder von der Verfügbarkeit eines Patches erhalten hat. Nach Abschluss der Beurteilung kann den Anwendern der betroffenen Produkte in den meisten Fällen normalerweise innerhalb von 3 bis 5 Arbeitstagen mitgeteilt werden, wie Philips auf das Problem reagieren wird.

Je nach Art der Bedrohung und des betroffenen Produkts kann eine validierte Korrektur oder ein Software-Update veröffentlicht werden. Wenn für die empfohlene Reaktion eine Änderung der Systemsoftware eines Medizingeräts erforderlich ist, kann ein Software-Update herausgegeben werden. Informationen hinsichtlich der Verfügbarkeit und Anwendbarkeit solcher Updates sind ebenfalls über die Standard-Kundendienstkanäle von Philips erhältlich und werden bei einigen Produkten in den sogenannten „Vulnerability Tables“ auf der Internetseite von Philips Healthcare aufgeführt.

Im Rahmen unserer Bemühungen, Ihnen diese wichtigen Informationen zeitnah und in praktischer Form zur Verfügung zu stellen, bietet die Internetseite von Philips Product Security nun Zugriff auf dynamische und produktspezifische Informationen zu Sicherheitslücken. Diese Daten werden in einfachen, produktspezifischen Tabellen aufbereitet, in denen die bekannten Software-Sicherheitslücken zusammen mit ihrem aktuellen Status, den empfohlenen Maßnahmen des Kunden, Tips und allgemeinen Anmerkungen aufgeführt sind.

Sie finden diese Informationen auf der Internetseite von Philips Healthcare Product Security:
http://www.healthcare.philips.com/main/support/productsecurity/vulnerability_tables.wpd

Wenn Sie Fragen zum Patch-Management oder zu den „Vulnerability Tables“ für Betriebssysteme haben, wenden Sie sich bitte per E-Mail unter *productsecurity@philips.com* an Philips Healthcare oder direkt an Ihren Philips-Kundendienstmitarbeiter.

Produktbeurteilung/Produktkonzeption

Philips Healthcare führt proaktiv interne Produktsicherheitsbeurteilungen durch, um potenzielle Sicherheitsschwachstellen zu identifizieren. Nach Auswertung dieser Daten definieren unsere Entwicklungsteams oftmals Konfigurationsänderungen und technische Anpassungen, mit denen das System besser vor äußeren Bedrohungen geschützt ist. Dieselben Informationen werden auch als Grundlage für die Anforderungen an das Sicherheitskonzept neuer Produkte genutzt. Die Philips-Produktsicherheitsrichtlinie verlangt, die Ziele der *Integrierten Sicherheit* bei der Konzeption aller neuen Produkte zu berücksichtigen.

Internetseite von Philips Product Security

Philips Healthcare stellt auf der Internetseite von Product Security verschiedenes Informationsmaterial für die Kunden bereit, darunter Sicherheits-Bulletins, FAQs, Informationen zu Sicherheitslücken, Links zu Branchenressourcen und andere Highlights aus dem Bereich Product Security.

MDS^2-Formulare

Um unsere Kunden in den USA bei der Einhaltung ihrer HIPAA-Verpflichtungen gemäß 2005 Security Rule zu unterstützen, hat Philips Healthcare eine Führungsrolle bei der Veröffentlichung von Produktsicherheitsinformationen übernommen[4]. Philips hat zahlreiche Maßnahmen ergriffen, um in Reaktion auf Kundenwünsche die Sicherheit unserer Medizingeräte zu optimieren. Bei ordnungsgemäßer Verwendung wird den Anwendern durch die Sicherheitsfunktionen von Philips Healthcare Produkten die Einhaltung ihrer Verpflichtung erleichtert, die Vertraulichkeit, Integrität und Verfügbarkeit von Gesundheitsdaten der Patienten zu gewährleisten. Angesichts der gesteigerten Bedeutung der Medizingeräte-Sicherheit und der Einhaltung der HIPAA Security Rule in den USA hat die Healthcare Information and Management Systems Society (HIMSS) ein Standarddokument „Manufacturer Disclosure Statement for Medical Device Security“ (MDS^2) erstellt. Das MDS^2 soll den Leistungserbringern wichtige Informationen zur Verfügung stellen, die sie dabei unterstützen können, die Sicherheitslücken und -risiken im Zusammenhang mit den elektronischen geschützten Gesundheitsdaten zu beurteilen, die von Medizingeräten erstellt, übertragen oder verwaltet werden.

Die MDS²-Formulare von Philips stehen unseren Kunden auf der Internetseite von Product Security zur Verfügung: *http://www.healthcare.philips.com/main/support/productsecurity/mds2.wpd*

Die Rolle des Kunden beim Thema Produktsicherheit Partnerschaft

Es ist uns bewusst, dass die Sicherheit von Philips Healthcare Produkten einen wichtigen Teil der detaillierten Sicherheitsstrategie Ihrer Einrichtung darstellt. Diese Vorteile können jedoch nur dann in vollem Umfang genutzt werden, wenn Sie Ihrerseits eine umfassende und mehrschichtige Strategie (mit Richtlinien, Prozessen und Technologien) implementieren, um die Daten und Systeme vor externen und internen Bedrohungen zu schützen. Nach der gängigen Industriestandard-Praxis sollte Ihre Strategie die Punkte physikalische Sicherheit, operationelle Sicherheit, Verfahrenssicherheit, Risikomanagement, Sicherheitsrichtlinien und Notfallpläne abdecken. Die praktische Implementierung der technischen Sicherheitskomponenten variiert je nach Standort und kann verschiedene Technologien beinhalten, z.B. Firewalls, Virenscanner-Software, Authentifizierungstechnologien usw. Wie bei jedem computerbasierten System muss durch die Schutzmaßnahmen gewährleistet sein, dass sich zwischen dem medizinischen System und allen Systemen, auf die extern zugegriffen werden kann, Firewalls und/oder andere Sicherheitsgeräte befinden. Die USA Veterans Administration hat zu diesem Zweck eine weit verbreitete Medical Device Isolation Architecture entwickelt[5]. Solche Perimeter- und Netzwerkverteidigungen sind unverzichtbare Elemente einer umfassenden Sicherheitsstrategie für Medizingeräte.

Richtlinien zu Drittanbieter-Software und Patching

Philips Healthcare vertreibt hochkomplexe Medizingeräte und -systeme. An diesen Systemen dürfen ausschließlich von Philips autorisierte Änderungen durchgeführt werden, die entweder von einem Philips-Mitarbeiter oder nach explizit von Philips veröffentlichten Anweisungen vorgenommen werden müssen. Angesichts des gegenwärtigen Anstiegs von Sicherheitsbedrohungen arbeiten die Philips-Produktentwicklungsteams daran, sicherheitsrelevante Drittanbieter-Software auf ausgewählten Geräten zu qualifizieren. Für uns genießen jedoch Patienten- und Anwendersicherheit nach wie vor höchste Priorität, und wir sind dazu verpflichtet, die behördlich regulierten Qualitätssicherungsverfahren zu beachten, um alle Änderungen am Betrieb unserer Medizingeräte zu verifizieren und zu validieren.

Philips Healthcare bietet ein breites Spektrum von Geräten an, von Bilderfassungs- und -anzeigesystemen über IT-orientierte PACS bis hin zu lebenswichtigen Rund-um-die-Uhr-Echtzeitmonitoren. Der sehr unterschiedliche Charakter unserer Produkte hat dazu geführt, dass wir verschiedene Formen der Installation und Wartung von Drittanbieter-Software unterstützen. Wenden Sie sich bitte an den Philips-Kundendienst, wenn Sie spezifische Informationen zu einem konkreten Produkt benötigen.

Allgemeinfall

Bei den meisten Geräten von Philips Healthcare darf ohne vorherige schriftliche Genehmigung keine Drittanbieter-Software jeglicher Art (z.B. Virenscanner, Office-Produktivitätstools, System-Patches, Firewalls auf der Plattform usw.) vom Kunden installiert werden. Bei nicht autorisierten Änderungen an Produkten von Philips Healthcare erlischt unsere Gewährleistung. Notwendige Kundendienstmaßnahmen, die auf solche Änderungen zurückzuführen sind, werden nicht von unseren Dienstleistungsverträgen abgedeckt. Solche Änderungen können die Leistung oder Sicherheit Ihres Geräts in unvorhersehbarer Weise beeinträchtigen. Philips übernimmt keine Verantwortung für Geräte, die eigenmächtig verändert wurden.

Wenn Philips den Einsatz von Virenscannern, System-Patches oder Upgrades autorisiert, erfolgt die Installation des Scanners/Patches/Upgrades in der Regel (1) durch Philips Healthcare zum Zeitpunkt der Herstellung oder Installation oder (2) nach der Installation durch einen von Philips zugelassenen Kundendiensttechniker.

Ausnahmen

Bei einigen wenigen Systemen erlaubt Philips die direkte Installation bzw. Aktivierung von Drittanbieter-Software durch Ihren zuständigen Philips-Systemadministrator, allerdings stets unter der Voraussetzung, dass die explizit von Philips Healthcare veröffentlichten Anweisungen befolgt werden, und nur bei den konkreten Systemen und Versionen, die von der schriftlichen Philips-Dokumentation abgedeckt sind.

Vor der Installation oder Aktivierung jeglicher Drittanbieter-Software auf einem Produkt von Philips Healthcare ist der für Sie zuständige Kundendienstmitarbeiter zu kontaktieren, um sich zu vergewissern, dass das fragliche Produkt für die betreffende Software qualifiziert wurde und, sofern dies der Fall ist, welche Einschränkungen ggf. gelten. Qualifikation und Nutzung dieser Softwareprodukte variieren je nach Philips-Produkt.

Es ist wichtig, dass Ihnen als unserem Kunden bewusst ist, dass jegliche nicht autorisierte Änderung eines medizinischen Geräts oder Systems von Philips (z.B. Änderung der Produkt-Firewall oder Installation von Patches, Viruserkennungssoftware, Dienstprogrammen, Spielen, Musikdateien, Updates usw.) unvorhersehbare negative Auswirkungen auf die Systemleistung oder -sicherheit haben kann, sodass Ihr Personal und Ihre Patienten nicht mehr von den Sicherheitsvorkehrungen geschützt sind, die von behördlicher Seite für Medizingeräte vorgegeben sind oder sich aus dem umfassenden Philips-Qualitätssystem für die Entwicklung, Herstellung und Prüfung unserer Geräte ergeben. Zu den möglichen schädlichen Begleiterscheinungen solcher Installationen oder Änderungen zählen unter anderem:

a) Die Öffnung oder Verbreiterung von Zugangsmöglichkeiten, durch die Zugriff oder Steuerung beeinträchtigt werden können
b) Die unsichtbare Einschleppung von Viren, Spyware, Trojanern, Backdoor-Zugangsmöglichkeiten oder anderen Remote-Agenten
c) Die Installation eines nicht autorisierten Updates, mit dem eine stabile Systemkomponente zu einer verwundbaren Komponente wird

Wenn Sie Kenntnis von einer nicht autorisierten Änderung an Ihrem Medizingerät oder -system von Philips haben oder eine solche vermuten, sollten Sie dies unverzüglich Ihrem Philips-Kundendienstmitarbeiter melden, der Sie dabei unterstützen wird, eine angemessene Abhilfemaßnahme festzulegen, mit der Ihr Gerät bzw. System wieder den Spezifikationen entspricht.

Philips Remote Service

Philips Healthcare hat ein globales, internetbasiertes Remote Services Network (RSN) eingerichtet, über das viele Ihrer Philips-Systeme mit unseren fortschrittlichen Service-Ressourcen verbunden werden können. Bei diesem hochmodernen System wird Ihr Gerät mit einem einzelnen Netzwerkzugriffpunkt über VPN-Technologien (Virtual Private Network) mit Philips-Geräten vor Ort verbunden. Dieses Secure-Tunnel-Konzept wurde mit dem Ziel entwickelt, eine Remote-Service-Lösung der Spitzenklasse bereit zu stellen, mit der die Verbindung über explizite Autorisierungs- und Authentifizierungskontrolle geschützt wird und alle Informationen in der Service-Sitzung verschlüsselt werden.

Philips Healthcare in einer sich verändernden Welt

Angesichts der Notwendigkeit, die Sicherheit unserer Medizinprodukte zu verbessern, wird Philips Healthcare weiterhin Überprüfungen und technische Anpassungen der bestehenden Produkte vornehmen, um die Anforderungen unserer auf Sicherheit bedachten Kunden in vollem Umfang zu erfüllen. Wir setzen alles daran, die Produkte von Morgen auf der Basis fundamentaler Sicherheitsprinzipien zu konzipieren. Wir werden auch weiterhin eng mit Ihrem Pflegepersonal und Ihren IT-Abteilungen zusammenarbeiten, um flexible Lösungen für aktuelle Probleme zu finden, während wir bereits an neuen Medizinprodukten mit *Integrierter Sicherheit* arbeiten. Wenn Sie Fragen zu unseren Bemühungen zur Verbesserung der Sicherheit unserer Produkte haben, können Sie sich gerne an Ihren Kundendienstmitarbeiter, Ihren Vertriebsmitarbeiter oder an *productsecurity@philips.com* wenden.

Vielen Dank für Ihr Interesse an den Philips Healthcare-Lösungen für den Gesundheitsbereich.

---

[1] Medical Device Security Workgroup der Healthcare Information and Management Systems Society (HIMSS) *http://www.himss.org/* siehe Topics and Tools >> Medical Device Security.

[2] IHE ist eine gemeinsame Initiative der Healthcare Information and Management Systems Society (HIMSS) und der Radiological Society of North America (RSNA) *http://www.ihe.net/*.

[3] Weitere Informationen siehe U.S. Food and Drug Administration Information for Healthcare Organizations about FDA's Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software unter *http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm*.

[4] Wenn Sie Exemplare des Dokuments „Manufacturer Disclosure Statement for Medical Device Security" (im MDS² -Standardformular der HIMSS) für Produkte von Philips anfordern möchten, besuchen Sie unsere Internetseite von Product Security unter *http://www.healthcare.philips.com/main/support/productsecurity/mds2.wpd*

[5] Siehe USA Department of Veterans Affairs Medical Device Isolation Architecture Guide, 30. April 2004, verfügbar auf der Internetseite von HIMSS unter *http://www.himss.org/ASP/topics_FocusDynamic.asp?faid=101*.

© 2010 Koninklijke Philips Electronics N.V.
Alle Rechte vorbehalten.

Philips Healthcare behält sich das Recht vor, ein Produkt zu verändern oder die Herstellung zu jedem Zeitpunkt und ohne Ankündigung oder Verpflichtung einzustellen.

Philips Healthcare ist ein Unternehmen der Royal Philips Electronics

www.philips.com/healthcare
healthcare@philips.com
fax: +31 40 27 64 887

Gedruckt in den Niederlanden
4522 962 17293 * FEB 2010