Johner Institut

Marktvorteile dank IT-Security

Mit Gerd Dautel, Prof. Dr. Christian Johner

Transkript

00:00:05 Sprecher 1

Medical Device Insights, ein Podcast des Johner Instituts für Medizinprodukteherstellen, Behörden und benannte Stellen.

00:00:17 Sprecher 1

Das Thema I.T.

00:00:19 Sprecher 1

Security werden wir wahrscheinlich auf längere Zeit nicht los.

00:00:22 Sprecher 1

Immer neue Datenskandale, Einbrüche und Angriffe beschäftigen

00:00:29 Sprecher 1

die IT-Unternehmen, aber auch alle anderen Branchen, auch das Gesundheitswesen.

00:00:33 Sprecher 1

Ein trauriges Beispiel war auch neulich der Angriff auf das Universitätsklinikum Düsseldorf, bei dem möglicherweise sogar eine Patientin durch diesen Angriff zu Tode kam.

00:00:45 Sprecher 1

Das heißt, wir Medizinprodukteherstellen müssen unseren Beitrag dazu leisten, sichere Produkte zu entwickeln.

00:00:53 Sprecher 1

Und heute im Gespräch habe ich jemanden dabei, der

00:00:56 Sprecher 1

eine Medizinprodukteherstellen arbeitet und sich um solche Produkte kümmert.

00:01:01 Sprecher 1

Das ist der Herr Daudel.

00:01:03 Sprecher 1

Herr Daudel, könnten Sie sich vielleicht als Person oder Ihre Rolle und die Produkte vorstellen, die Sie herstellen?

00:01:10 Sprecher 1

Ich glaub, das wird uns einen guten Kontext geben, über was wir heute sprechen.

00:01:14 Sprecher 2

Ja, hallo, erstmal vielen Dank für die Einladung.

00:01:17 Sprecher 2

Ich bin Gerd Daudel, vom Hintergrund bin ich Medizin Informatiker

00:01:24 Sprecher 2

und bin bei der Firma Streiter tätig und da als Leiter fürs Qualitätsmanagement und Zulassungswesen und das schon seit geraumer Zeit.

00:01:33 Sprecher 2

Und ich befasse mich mittlerweile seit etwa 4 Jahren mit Cybersecurity.

00:01:39 Sprecher 2

Wir hatten im Konzern zum Ziel, Cybersecurity-Maßnahmen quasi auf Konzernebene, auf konzernweite Standards zu heben, also raus aus den Projekten, rein ins Corporate Qualitätsmanagementsystem.

00:01:53 Sprecher 2

und die so zu harmonisieren und zu integrieren, dass wir auch für unsere digitale Zukunft sozusagen gerüstet sind.

00:02:01 Sprecher 2

Striker ist ‚n reiner Medizinprodukteunternehmer, ‚ne reine Medizinproduktefirma.

00:02:06 Sprecher 2

Wir machen von Implantaten bis vernetzte Produkte, haben wir ‚n ganz großes Spektrum.

00:02:12 Sprecher 2

Wenn man über vernetzte Produkte redet, kann man vielleicht unsere Navigationssysteme erwähnen, die vernetzt sind, aber wir machen auch so was wie Defibrillatoren,

00:02:22 Sprecher 2

die netzwerkfähig sind oder Krankenhausbetten, die vernetzt sind und vieles andere mehr.

00:02:30 Sprecher 1

Das heißt, Sie haben auf der einen Seite vernetzte Produkte und auf der anderen Seite Produkte, die besonders ja sicherheitsrelevant sind.

00:02:38 Sprecher 1

Sie sprachen jetzt gerade über Navigationssysteme und über Defibrillatoren.

00:02:42 Sprecher 1

Ich glaub, da liegt es auf der Hand, welche Bedeutung ‚ne gute I.

00:02:45 Sprecher 1

T.

00:02:46 Sprecher 1

Security hat.

00:02:47 Sprecher 1

Was tun Sie in Ihrem Unternehmen, um die Cybersecurity

00:02:51 Sprecher 1

zu gewährleisten und wer spielt da alles mit, also welche Rollen führen da welche Aktivitäten aus?

00:02:58 Sprecher 2

Ja, ich hab es gerade erwähnt, auf der einen Seite haben wir auf der Ebene des Qualitätsmanagementsystems, des Tryker Qualitätsmanagementsystems, verschiedenste Prozeduren implementiert, da speziell im Design for Security, also wie muss ich Security implementieren im Entwicklungsprozess.

00:03:19 Sprecher 2

Eine andere große Frage war, wie kann ich Security-Risikomanagement harmonisieren mit dem Risikomanagement auf 14 971 also dem Gesundheitsschutz, wenn man so will.

00:03:31 Sprecher 2

Und ‚n großes anderes Themengebiet war Post-Market-Management.

00:03:35 Sprecher 2

Was bedeutet Cybersecurity, wenn die Produkte auf dem Markt sind, wie mache ich da die Überwachung, auf welche Kanäle muss ich gucken und all so was.

00:03:44 Sprecher 2

Um all dieses hinzubekommen, haben wir

00:03:48 Sprecher 2

waren wir organisatorisch tätig, wenn man so will.

00:03:51 Sprecher 2

Wir haben ‚ne zentrale ‚n zentrales Kernteam eingerichtet, was in ständigem Kontakt mit dem Management von unseren Divisionen steht, um zum Beispiel im monatlichen Rhythmus Pläne zu besprechen, wie man da weiter vorgeht.

00:04:09 Sprecher 2

Wir haben aber auch Spezialisten oder Fokusgruppen eingerichtet, die sich eben um die 3 Themengebiete, die ich gerade erwähnt hab, noch mal Design and Privacy for Security, Risk Management for Security und Post Market Management kümmern.

00:04:24 Sprecher 1

Könnten Sie uns ,n paar Beispiele dafür geben, was Sie im Bereich Design machen?

00:04:29 Sprecher 1

Also ich keine Geheimnisse, aber sozusagen generelle Überlegungen, die Sie da treffen und

00:04:35 Sprecher 1

ganz grob vielleicht Maßnahmen, die sie dabei ergreifen.

00:04:37 Sprecher 2

Ja, eine eine der ersten Überlegungen vor Jahren war, als ich damit eingestiegen bin.

00:04:43 Sprecher 2

Gibt es irgendwelche Kataloge, die man hernehmen kann, um User-Needs in dem Fall Security Needs zu verstehen und wie kann man die unterfüttern und wie kann man die ankurbeln an den Softwareentwicklungsprozess, den wir natürlich schon lange etabliert haben.

00:04:58 Sprecher 2

Was bedeutet es dann auch für die Architektur und fürs Design, wie wir das weiter verfeinert

00:05:04 Sprecher 2

und in welchem Zusammenhang steht es mit dem mit dem Cybersecurity Risikomanagement.

00:05:10 Sprecher 2

Wir verstehen das mittlerweile als iterativen Prozess, also was wir da gemacht haben, ich fang noch mal vorne an bei den Cybersecurity Needs und bei den Cybersecurity Spezifikationen, wenn man so will.

00:05:22 Sprecher 2

Da gibt es Kataloge dazu, die finden sich in verschiedenen Standards, das nennt sich dann Capabilities zum Beispiel.

00:05:29 Sprecher 2

es sind Kategorien zu Cybersecurity, auf die man achten kann in dem Zusammenhang, die weiter runtergebrochen sind in sogenannte Controls.

00:05:38 Sprecher 2

Das sind spezifischere Anforderungen.

00:05:40 Sprecher 2

So was wurde implementiert in unser allgemeines Design-Input-Gerüst.

00:05:44 Sprecher 2

Also ich rede bisschen amerikanisch, weil ich halt immer amerikanische Konzern bin.

00:05:48 Sprecher 2

Ich hoffe, dass es trotzdem verstanden wird.

00:05:51 Sprecher 1

Absolut.

00:05:52 Sprecher 1

Wenn Sie uns vielleicht doch ‚n Beispiel für einen Need und ein Control geben könnten, dann wären wir noch sicherer,

00:05:58 Sprecher 1

Dass alle Hörer sozusagen auch das gleiche mentale Modell haben.

00:06:02 Sprecher 2

Ja, man will ja nicht, dass wenn ein Rechner irgendwo in einer in der Praxis steht, zum Beispiel, oder auf einer Station in der Klinik, dass der, wenn derjenige, der sich damit grad befasst hat, wenn der aufsteht und geht, dass die jeder andere dran kann.

00:06:19 Sprecher 2

Also, so eine Capability oder so, need wer ein Outlook of.

00:06:22 Sprecher 2

eine Controlware, welche Funktionen müssen sozusagen eingeschaltet werden, um dieses Auto-Lock-off nach einer bestimmten Zeit zum Beispiel sicherzustellen, dass er sich nach einer Minute, nach 2 Minuten oder wie auch immer quasi abschalten.

00:06:37 Sprecher 2

Anderes Beispiel wäre, es geht irgendjemand anderer dran, ja wie sieht es jetzt aus, dass wenn der jetzt 345 mal versucht da einzudringen, dass man das halt verhindern kann?

00:06:48 Sprecher 1

Mhm.

00:06:49 Sprecher 1

und dann entsprechend wieder das Control, die Maßnahme implementiert, die das erkennt und dann entsprechend reagiert.

00:06:55 Sprecher 1

Sie haben jetzt schon ziemlich klar gemacht und das finde ich sehr wichtig, dass dieses Thema I.

00:07:01 Sprecher 1

T.

00:07:01 Sprecher 1

Security eigentlich ein komplettes Lifecycle Thema ist, also die alle Phasen der Entwicklung, aber eben auch danach umfasst und in dem Kontext haben Sie bereits

00:07:11 Sprecher 1

den Begriff der Post-Market Surveillance oder Post-Market Aktivitäten mit erwähnt.

00:07:17 Sprecher 1

Was machen Sie in diesem Bereich, also nach Inverkehrbringung der Produkte, um die I.

00:07:23 Sprecher 1

T.

00:07:23 Sprecher 1

Sicherheit Ihrer Produkte langfristig zu gewährleisten.

00:07:26 Sprecher 2

Ja, Sie müssen erstmal verstehen, aus welchen Kanälen, Informationsquellen, sozusagen Vulnerabilities noch mal im Amerikanischen, also potentielle Schwächen, die ihre Produkte, ihre netzwerkfähigen Produkte betreffen,

00:07:40 Sprecher 2

aus welchen Kanälen soll solche Informationen kommen können.

00:07:45 Sprecher 2

Typischerweise als Medizinproduktehersteller kennt man das Complaint Handling oder sie kennen ein Non-Conformity Kappa System und all so was.

00:07:53 Sprecher 2

Ja, aber in dem Fall spielt auch die Öffentlichkeit, Medien zum Beispiel, so eine große Rolle.

00:07:58 Sprecher 2

Man denke da an WannaCry.

00:08:01 Sprecher 2

Vielleicht kennt man das, WannaCry war ‚ne Ransomware Attack,

00:08:05 Sprecher 2

die große Teile des englischen Gesundheitssystems lahmgelegt hat.

00:08:09 Sprecher 2

Das war etwa vor zweieinhalb Jahren, wenn ich mich recht entsinne.

00:08:12 Sprecher 2

Ja, auf sowas gilt es zu überwachen und dann gibt es mittlerweile auch Datenbanken, die öffentlich zugänglich sind, die zum Beispiel regelmäßig aktualisieren, welche Schwächen, welche Schwächen auf Windows 10 zum Beispiel zutreffen, welche Patches eingespielt werden müssen und sowas gilt es auch zu überwachen.

00:08:30 Sprecher 2

Insgesamt ist das ein relatives komplexes Geschehen.

00:08:34 Sprecher 2

und deshalb kann man sich und muss man sich wahrscheinlich auch überlegen, ob man da die Tools zu Hilfe nimmt.

00:08:39 Sprecher 2

Da gibt es Tools wie zum Beispiel Black Duck, die solche Datenbanken quasi überwachen, wenn die denn wissen, welche Komponenten in ihre Software integriert sind.

00:08:49 Sprecher 1

Ja, das spellen jetzt wahrscheinlich auch auf die NIST Datenbank an, die ja mit mehreren 1000 Meldungen pro Monat da den manchen überfordern mag.

00:09:00 Sprecher 1

und da helfen solche Werkzeuge wie das Black Duck, was Sie gerade erwähnt haben, oder auch unsere Post-Market Radars, genau sowas zu überwachen, eben die ganze Breite an Informationsquellen, die Sie gerade geschildert haben.

00:09:15 Sprecher 1

Das hört sich jetzt so an, als ob man doch einige Ressourcen dazu braucht, also jetzt nicht nur mengenmäßig, sondern auch bezüglich der Kompetenzen.

00:09:25 Sprecher 1

Jetzt ist Stryker ein sehr großer Hersteller,

00:09:28 Sprecher 1

Was würden Sie anderen Herstellern empfehlen und wann denken Sie, wär es notwendig, dass die auch externe Hilfe in Anspruch nehmen?

00:09:36 Sprecher 2

Ja, ich kann vielleicht von mir reden, als ich vor 4 Jahren etwa damit anfing und gefragt wurde, ob ich da helfen kann, das Corporate-Wide zu etablieren, also Cybersecurity-Management und integrieren in unsere, in unser Corporate-Qualitätsmanagement,

00:09:53 Sprecher 2

da hatte ich so ‚ne Vorstellung wie vor etwa 10 Jahren, hab ich als ich was Ähnliches gemacht hab für die 14 971 14 971 also das Gesundheitsrisikomanagement, wenn man das so abgrenzen kann zu Cyber Security Risikomanagement.

00:10:07 Sprecher 2

Was ich halt erlebt hab, ist ‚ne Fülle von Standards, von Guidances.

00:10:12 Sprecher 2

Also ich hab gestern das mal kurz überschlagen, ich hab

00:10:15 Sprecher 2

mittlerweile deutlich über 100 Standards in Guidances, die ich mehr oder weniger gründlich gelesen hab.

00:10:20 Sprecher 2

Was ich damit sagen will, ist ‚n ziemlich anspruchsvolles Gebiet und ‚n relativ komplexes Gebiet.

00:10:26 Sprecher 2

Also, wo jemand schon mal helfen kann, ist beim Einstieg überhaupt Orientierung zu zu geben, wo muss ich da, wo muss ich dahin hin fassen, was lese ich mal durch, was ist relevant für mich, was bedeutet Integration für meinen speziellen Kontext, also welche Art von Medizinprodukt mache ich und

00:10:45 Sprecher 2

Was bedeutet das dann für mein Qualitätsmanagementsystem Cybersecurity?

00:10:49 Sprecher 2

Was übrigens noch dazukommt in Europa ist die Datenschutzgrundverordnung.

00:10:55 Sprecher 2

Also, was man gleichzeitig machen sollte, sind meines Erachtens sind Datenschutzgrundverordnungen, Anforderungen gleich mitdenken, weil Cybersecurity ist für mich ‚ne notwendige Voraussetzung für Datenschutz, aber keine hinreichende.

00:11:07 Sprecher 2

Deshalb muss ich das mitdenken, meiner Ansicht nach.

00:11:09 Sprecher 1

Sie haben jetzt schon gesagt, dass Sie Hilfe dann empfehlen würden, um überhaupt ins Thema reinzukommen, um ‚n Überblick zu erreichen, welche Best Practices, Standards, Normen und so weiter.

00:11:21 Sprecher 1

existieren und welche von denen es auch wert sind, da näher studiert zu werden.

00:11:25 Sprecher 1

Wenn wir der Technik ‚n bisschen weiter runter gehen, also beispielsweise Kodierstandards, Penetration Testing, Fast Testing, würden Sie solche Aktivitäten auch nach außen geben oder ist es was, was Sie sagen, nee, das gehört ins Unternehmen rein.

00:11:40 Sprecher 2

Es kommt drauf an, es bedarf einiges, einiges an Kompetenz und an Wissen.

00:11:48 Sprecher 2

wenn man das selber aufbauen muss, noch mal, ich glaube wirklich, das ist ‚n komplexes Thema, dann braucht man ‚ne Weile, um auf Stand zu kommen.

00:11:56 Sprecher 2

Also bietet es sich an, das nach außen zu geben, um ‚n Beispiel aus der eigenen Organisation zu geben, es zu zeigen, wir sind gerade dabei, weltweit zentralen Testlabor genau für diese Art von Test zu etablieren.

00:12:08 Sprecher 2

Genau aus dem Grund, weil wir verhindern wollen, dass man das Rad immer wieder neu erfindet und damit auch die inkonsistenten der Herangehensweise sozusagen erzeugt.

00:12:17 Sprecher 1

Und da wird auch, denk ich, klar, da braucht man ‚ne gewisse Größe, damit sich das auch rechnet, ‚ne Infrastruktur, ‚n Personalstamm aufzubauen, der nicht nur in der Lage ist, sich in diese Themen einzuarbeiten, sondern auch in der Lage ist, da mit dem Stand der Technik Schritt zu halten.

00:12:35 Sprecher 1

Ja, jetzt haben Sie schon über Normen, über Standards, über Best Practices gesprochen gehabt.

00:12:40 Sprecher 1

Sie haben gesagt, es sind

00:12:42 Sprecher 1

einige 100, Was sind so die wichtigsten, an denen sie sich orientieren oder von denen sie der Meinung sind, dass man sie schon mal nicht nur kennen, vielleicht sondern auch gelesen haben sollte?

00:12:52 Sprecher 2

Ja, es gibt 2 wesentliche von der F.D.A., die schon seit einigen Jahren publiziert sind, nämlich die, die es gibt 2 Guidances von der F.D.A., einmal zu Design Controls, also welche Unterlagen zu Cybersecurity werden erwartet bei der Zulassung von Medizinprodukten in den U.S.A.

00:13:10 Sprecher 2

Das wäre das eine

00:13:11 Sprecher 2

und die andere Guidance bezieht sich auf Post-Market, Post-Market Surveillance und das Risikomanagement für Produkte, die schon auf dem Markt sind und das verbunden auch mit Meldepflicht in den U.

00:13:22 Sprecher 2

S.

00:13:22 Sprecher 2

A.

00:13:23 Sprecher 2

übrigens auch ‚n ganz interessanter Aspekt.

00:13:25 Sprecher 2

Wenn man zurückkehrt in den Entwicklungsprozess selber, dann haben wir uns orientiert an einigen I.

00:13:31 Sprecher 2

E.

00:13:32 Sprecher 2

C.

00:13:32 Sprecher 2

und NIST Standards.

00:13:33 Sprecher 2

Ich hab von den Capabilities schon geredet oder den Cybersecurity User Needs,

00:13:39 Sprecher 2

da hilft ,n Standard wie die I.E.C.

00:13:41 Sprecher 2

800001 strich 2 strich 2 die Listed Capabilities oder diese Kategorien von Cybersecurity.

00:13:49 Sprecher 2

Und wenn sie dann noch in den NIST Standard 800 strich 53 reinschauen, dann kriegst du die ganzen Controls, die diese etablieren wollen, um diese Capabilities sozusagen mit mit mit Leben zu füllen, wenn man so will.

00:14:06 Sprecher 2

Beim Risikomanagement

00:14:09 Sprecher 2

Wäre wichtig, dass man sich mit dieser mit mit einer AMI Guidance beschäftigt, die der T.I.R.

00:14:16 Sprecher 2

57, die beschreibt Principles for Medical Device Security und wo die ,n ganz guter Job macht, meiner Ansicht nach, ist im Grunde die Darlegung, wie Cybersecurity, Risikomanagement und Safety-O-Health-Risk-Management, wie die, wie man die in Gleichklang bringen kann.

00:14:34 Sprecher 1

Ja, das halte ich für sehr ganz wichtigen Ergänzung, die Sie hier machen, weil viele dieser Guidances ja als Endpunkt die I.

00:14:42 Sprecher 1

T.

00:14:42 Sprecher 1

Security haben, also die Fähigkeit, Informationen und Informationstechnik zu schützen und deren die Vertraulichkeit, die Integrität und die

00:14:55 Sprecher 1

Verfügbarkeit von eben Informationen, Informationstechnik zu gewährleisten.

00:14:59 Sprecher 1

Aber für uns Medizinproduktehersteller ist das ja nicht der Endpunkt oder nicht der einzige.

00:15:03 Sprecher 1

Wir haben immer die Safety, die wir letztlich im Kopf behalten müssen.

00:15:07 Sprecher 1

Ja, aber damit haben Sie uns schon mal diese unendlich große Liste doch sehr reduziert.

00:15:12 Sprecher 1

Ich glaub, das wird sehr hilfreich sein.

00:15:14 Sprecher 1

Wir haben in den Begleitmaterialien, haben wir auch noch ein

00:15:18 Sprecher 1

Artikel mit aufgeführt, bei denen Sie ‚ne Übersicht über all diese Normen und Standards bekommen und da sind auch die eben genannten mit erwähnt, mit kommentiert und ich glaub, die sind ziemlich wichtig, die Sie hier gerade genannt haben.

00:15:33 Sprecher 1

Wir haben gerade eben schon gesprochen gehabt über das Thema Outsourcing von gewissen I.

00:15:38 Sprecher 1

T.

00:15:39 Sprecher 1

Security Aktivitäten.

00:15:41 Sprecher 1

Ich möchte noch mal zur zum Outsourcing kommen, aber dieses Mal ‚n bisschen aus einer anderen Brille.

00:15:46 Sprecher 1

Viele Hersteller

00:15:47 Sprecher 1

entwickeln ja die Software gar nicht notwendigerweise selber, sondern nutzen dafür selber wiederum Entwicklungsdienstleister.

00:15:55 Sprecher 1

Was würden Sie empfehlen, was ein Hersteller, also ein Inverkehrbringer, tun sollte, um die I.

00:16:01 Sprecher 1

T.

00:16:01 Sprecher 1

Sicherheit seiner Produkte auch dann zu gewährleisten, wenn diese Software von dem dritten Partner hergestellt wird?

00:16:09 Sprecher 1

Also sozusagen, welche

00:16:11 Sprecher 1

Lenkung dieser Prozesse empfehlen Sie da.

00:16:13 Sprecher 2

Ja, da muss man bisschen in die Bücher gucken, glaube ich.

00:16:15 Sprecher 2

Also, wie gut ist der Hersteller gerüstet, um Cybersecurity tatsächlich rein zu designen in die Produkte.

00:16:23 Sprecher 2

Und da bin ich auf ihren ihren Leitfaden gestoßen für I.

00:16:27 Sprecher 2

T.

00:16:27 Sprecher 2

Security vor einiger Zeit und den verwende ich tatsächlich im Moment.

00:16:31 Sprecher 2

Genau in so einer Beziehung zum Lieferant von Software, die wir halt gern als O.

00:16:35 Sprecher 2

E.

00:16:36 Sprecher 2

M.

00:16:36 Sprecher 2

Produkt einsetzen würden.

00:16:38 Sprecher 2

und der ist in dem Zusammenhang auch wirklich, wirklich, wirklich hilfreich und sinnvoll, weil er halt die verschiedensten Aspekte harmonisiert und zusammenbringt in einer Checkliste, die man einfach ab-arbeiten kann.

00:16:52 Sprecher 2

Was mir auch gut gefällt, ist das Reifegradmodell, was sie da rein designt haben, also diese Stufen von 0 bis 2, was brauche ich mindestens, wo bin ich schon ganz gut und was wäre sozusagen best in class.

00:17:05 Sprecher 2

Es gibt übrigens was Ähnliches, bisschen länger schon auf dem Markt.

00:17:10 Sprecher 2

Es gibt diesen Medical Device and Health I.T.

00:17:13 Sprecher 2

Joint Security Plan.

00:17:14 Sprecher 2

Ich weiß nicht, ob Sie den kennen.

00:17:16 Sprecher 2

Der wurde Anfang 2019 herausgegeben von der Healthcare und Public Health Sector Organisation in U.S.A.

00:17:26 Sprecher 2

Das ist ein Konglomerat aus F.D.A.

00:17:30 Sprecher 2

Medizinprodukte, Industrie und und und Beratungsfirmen.

00:17:36 Sprecher 2

Die beschreiben in dem in in dieser Guidance ‚n ganz schönes, finde ich, holistisches Bild zu Cybersecurity und Medizinprodukte und übrigens auch Health I.

00:17:46 Sprecher 2

T., was ich interessant finde in dem Zusammenhang.

00:17:49 Sprecher 2

Der kapriziert sich nicht nur auf Medizinprodukte, sondern nimmt auch Health I.

00:17:53 Sprecher 2

T.

00:17:53 Sprecher 2

ins Scope, was ich wichtig finde, weil man so was schnell abschneidet.

00:17:57 Sprecher 2

Und da findet sich auch so ‚n Art Assessment Vorgehen, was sich auf C.M.M.I.s stützt.

00:18:04 Sprecher 2

also dieses Reifegradmodell, was von der Carnegie Meln Universität kommt, ist ‚n bisschen kürzer.

00:18:09 Sprecher 2

Wenn man es also kürzer und schneller haben will, zum Beispiel für für sich selber, wo steh ich heut mit meinem Cybersecurity Qualitätsmanagementsystem, kann das ganz hilfreich sein, was da drin steht.

00:18:20 Sprecher 1

Absolut und ich denk, wir werden in beide Dokumente, das von der, also dieses Reifegradmodell und den I.

00:18:27 Sprecher 1

T.

00:18:27 Sprecher 1

Security Leitfaden, den wir

00:18:29 Sprecher 1

die am Jona Institut entwickelt haben und übrigens auch die benannten Stellen weitergeführt haben, werden wir in beides verlinken.

00:18:36 Sprecher 1

Soweit haben wir jetzt die Cybersecurity eher unter einem Aspekt uns angeschaut gehabt.

00:18:41 Sprecher 1

Ja, wir müssen die Produkte sicher bauen und da schwingt so ein bisschen mit, an und für sich kann man bei diesem Thema nur verlieren.

00:18:48 Sprecher 1

Also im besten Fall hat man eben kein I.

00:18:51 Sprecher 1

T.

00:18:51 Sprecher 1

Security Problem und im anderen Fall hat man 1, aber richtig gewinnen kann man mit diesem Thema nicht.

00:18:56 Sprecher 1

Oder haben Sie ,ne Idee, wie man

00:18:59 Sprecher 1

bei dem Thema I.

00:19:00 Sprecher 1

T.

00:19:00 Sprecher 1

Security vielleicht sich sogar ,n Marktvorteil verschaffen kann.

00:19:03 Sprecher 2

Ja, das das sehen wir tatsächlich schon in U.

00:19:06 Sprecher 2

S.

00:19:06 Sprecher 2

A.

00:19:07 Sprecher 2

Also, das ging schon vor Jahren los, als ich ins Thema eingestiegen bin, dass immer mehr Kunden, also Kliniken oder Einkaufsgesellschaften, Darlegung für Cybersecurity gefordert haben.

00:19:20 Sprecher 2

Also ganz zu schweigen, ich rede jetzt wieder über ‚ne amerikanische Marktform, die Department of Defense, was zusammen mit der schon genannten Carnegie Mellon University

00:19:29 Sprecher 2

also wirklich ganz gehobene Standards, was Cybersecurity angeht, einfordert.

00:19:34 Sprecher 2

Wir, wir standen schon vor der Situation, dass wir wirklich um Aufträge gekämpft haben, weil weil die Darlegung nicht gleich da war, wenn man so will, was Cybersecurity angeht.

00:19:49 Sprecher 2

Das

00:19:50 Sprecher 2

Also und und ich hab es vorhin erwähnt, wir sind, wir sind auch natürlich mit mit Einkaufsgesellschaften, großen Einkaufsgesellschaften für Medizinprodukte in U.

00:20:01 Sprecher 2

S.

00:20:01 Sprecher 2

A.

00:20:02 Sprecher 2

in Kontakt.

00:20:02 Sprecher 2

Die fordern nicht nur die Darlegung von Cybersecurity, was konkrete Produkte angeht, zum Beispiel mithilfe von einer M.

00:20:09 Sprecher 2

D.

00:20:09 Sprecher 2

S.

00:20:10 Sprecher 2

Square Form oder M.

00:20:11 Sprecher 2

D.

00:20:11 Sprecher 2

S.

00:20:11 Sprecher 2

2 Form, die auf strukturierte Art und Weise so ‚ne Art Fragebogen

00:20:16 Sprecher 2

bietet, wo sie mit Ja-Nein halt beantworten können, welche Elemente dafür, also für das spezifische Produkt relevant sind, sondern die formulieren Cybersecurity-Anforderungen in die Verträge rein, in die grundsätzlichen Verträge rein.

00:20:31 Sprecher 1

Sie haben mir, glaube ich, sehr klar gemacht, dass da mit Cybersecurity nicht nur ‚ne regulatory Anforderung ist, sondern auch ‚ne Marktanforderung.

00:20:39 Sprecher 1

Das heißt, da bekommen die Hersteller letztlich von 2 Seiten Druck.

00:20:43 Sprecher 1

Ja, vielen Dank, Herr Daudel,

00:20:45 Sprecher 1

dass sie uns diese Einblicke gewährt haben, dass sie uns gezeigt haben, ja, welche Aktivitäten bei ihnen durchgeführt werden, dass sie wichtige Dokumente für uns genannt haben, dass sie uns auch nicht nur sozusagen auf die Pre-Market-Seite aufmerksam gemacht haben, sondern eben auch auf die Post-Market-Aktivitäten.

00:21:06 Sprecher 1

und die Leitfäden, die wir da einsetzen können, um diesen regulatorischen und Marktanforderungen möglichst elegant gerecht zu werden.

00:21:14 Sprecher 1

Vielen Dank, Herr Daudel, dass Sie dabei waren.

00:21:16 Sprecher 2

Ja, ich danke Ihnen.

00:21:17 Sprecher 2

Schönen Tag noch.

00:21:18 Sprecher 2

Vielen Dank.