ExperSite

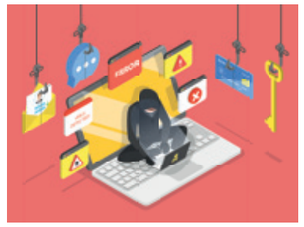
Ausgabe 01 | 2023

Das Magazin für Digitalisierung, Informationssicherheit und Datenschutz

Betriebsfähigkeit für Unternehmen im Notfall:

HÖRT AUF EUCH ZU BESCHWEREN!

Warum Informationssicherheit und Datenschutz Teil der guten Vorsorge sind



Exper*Site* ist das Magazin der JÄSCHKE GRUPPE für Digitalisierung, Informationssicherheit und Datenschutz

JÄSCHKE GRUPPE
GEMEINSAM DIGITALISIERUNG LEBEN

www.dr-jaeschke.ag

Zur JÄSCHKE GRUPPE gehören die Unternehmen:

DATATREE YOUR COMPLIANCE PROVIDER

GAIMS Information Security

puravivo

DIGITAL AVANTGARDE

MEMO

Business Continuity Management, oder: Das Ändern von Machtverhältnissen

Informationssicherheit, Datenschutz, Cyber-Security, IT-Sicherheit... die Liste dieser Begriffe ist lang und sie alle haben etwas gemeinsam - all diese Themen sind Grundlage für eine erfolgreiche Digitalisierung, unabhängig von Branche und Unternehmensgröße. Und auch wenn das KHZG einen Aufschwung in die zögerliche Investitionskultur des deutschen Gesundheitswesens brachte und auch IT-Sicherheit hier verpflichtende Voraussetzung für jegliche Investitionsvorhaben darstellt, so existiert häufig noch ein grundlegendes Mindset Problem.

Es gibt noch immer ein Mindset-Problem.

Um es einmal sinnbildlich zu betrachten: Was bringt es, wenn wir ein Sicherheitsschloss an unserer Haustür installiert haben, allerdings die Fenster alle sperrangelweit offenstehen? So sieht in vielen Fällen die Praxis aus. Wenn dann ein unbefugter Dritter Zugang zu unserem Haus erlangt und von innen alle Fenster schließt, ändert sich das Machtverhältnis der Beteiligten. Einig können wir uns darüber sein, dass es grundlegenden Voraussetzungen bedarf, um die Fenster schließbar zu gestalten und ggf. andere Sicherheitslücken zu identifizieren. Nur so können wir uns potenziellen Risiken darstellen, Versicherungen abschließen und uns auf den Notfall vorbereiten.

Und auch wenn Sie diese Versinnbildlichung weit hergeholt empfinden, lässt sie sich relativ einfach auf die Informations- und IT-Sicherheit übertragen. Wir haben das große Ziel, den Geschäftsbetrieb auch in Notsituationen aufrecht zu erhalten und beschäftigen uns daher in dieser Ausgabe mit dem Thema Business-Continuity Management, geben Ihnen praktische Umsetzungshilfen und stehen Ihnen mit unserer Berater:innen-Expertise jederzeit zur Seite.

Ich wünsche Ihnen viel Freude, Inspiration und den ein oder anderen Erkenntnisgewinn beim Lesen dieser Ausgabe.

Ihre Nina Kill
(Redaktionsleitung)

Hört auf Euch zu beschweren!

„Vorsorge ist besser als Nachsorge“ – das gilt nicht nur für die menschliche Gesundheit, sondern auch für das unternehmerische Wohlergehen von Kliniken und anderen Leistungserbringer:innen. Zahlreiche Vorfälle aus der Vergangenheit zeigen, wie fatal die Auswirkungen eines Cyberangriffs auf die komplette Versorgungskette sind.

Text: Nina Khan

Wie gefährdet eine Organisation ist und wie hoch der potenzielle Schaden im Ernstfall wird, kann im Vorfeld im Rahmen des Business Continuity Managements (BCM) ermittelt werden. Die Erkenntnisse dienen der Maßnahmenplanung für die Aufrechterhaltung des Betriebs trotz Notfallsituation.

Besonders im Gesundheitswesen ist die Gefährdung von sensiblen Informationen und Prozessen aufgrund der Kritikalität als Leistungserbringer:in durch einen Cyberangriff mit drastischen Folgen verbunden – die Informationssicherheit in Digitalisierungsprojekten muss deshalb von Beginn an zum Standard werden.

Stattdessen sind die Beschwerden nach wie vor laut, Informationssicherheit und Datenschutz gelten als Verhinderer und als Grund für das Scheitern der Projekte - ein unsachgemäßer Vorwurf, der sich jedoch hartnäckig hält.

Das Jahr 2022 neigte sich bereits dem Ende zu, als die Meldung aus dem Klinikum Lippe sämtlichen Akteuren aus dem Gesundheitswesen den Atem stocken ließ: Ein massiver Cyberangriff führte zu Teilausfällen der IT an allen drei Standorten in Detmold, Lemgo und Bad Salzuflen. Das Landeskriminalamt, Ermittelnde aus Bielefeld und Köln, externe Cybersicherheits-Dienstleister:innen sowie eine Wirtschaftsprüfungsgesellschaft schritten ein, um gemeinsam durch Abwehrmaßnahmen den Angriff abzuwenden. Später hieß es, dass die Entschlüsselung der Systeme durch intensive Verhandlungen mit den Erpresseri:innen gelungen sei. Die IT-Infrastruktur wurde heruntergefahren, IT-Systeme neu aufgesetzt. Zwei Wochen lang konnte das Klinikum nur per Telefon oder Fax kontaktiert werden. Allerdings seien zu keiner Zeit Patient:innen gefährdet gewesen.

Anders war das bei einem Angriff zwei Jahre zuvor auf eines der größten Krankenhäuser in Nordrhein-Westfalen, dem Universitätsklinikum Düsseldorf, bei dem Daten von 30 Servern durch Hacker verschlüsselt wurden. Die Folge war das Albtraumszenario eines jeden Klinikums: Operationen und Behandlungen fielen aus, Ambulanzen und Notaufnahmen mussten schließen. Aus einem Erpresserschreiben ging hervor, dass die Attacke eigentlich der Heinrich-Heine-Universität galt. Nachdem die Ermittler:innen den Hackern mitteilten, ein falsches Angriffsziel getroffen zu haben, wurde der Entschlüsselungscode kommuniziert. Dennoch dauerte es mehrere Wochen, bis der Krankenhausbetrieb wieder normal lief. Frank Schneider, der Ärztliche Direktor der Klinik, teilte dem WDR damals mit:

> Keine Notarztwagen, keine Hubschrauber, keine Krankenwagen kamen mehr, alle Ambulanzen waren geschlossen. Das ist eine schreckliche Zeit gewesen für uns und die Patient:innen.

Die Liste der Cyberangriffe lässt sich im jungen Jahr 2023 problemlos weiterführen: Der Dienstleister von Sozialversicherungsträgern BITMARCK bestätigte im Januar den unbefugten Zugriff auf die IT-Infrastruktur, ebenso wie der IT-Dienstleister adesso. Kurz darauf berichteten Medien von einer globalen Hackerattacke durch eine IT-Sicherheitslücke, bei der Hunderte Firmen, darunter auch deutsche, von Erpressersoftware betroffen waren.

Höher, weiter, Ransomware

Während Künstliche Intelligenz die Medizin revolutioniert, beispielsweise durch die Analyse von Röntgen und Ultraschallbildern und KI-Projekte damit weitreichenden Einfluss in die Diagnostik und den Behandlungsverlauf nehmen, sind Informations- und IT-Sicherheit die unliebsamen Stiefschwestern der Digitalisierungsprojekte. Selbiges gilt für Dienstleister:innen und Leistungserbringer:innen. Scharfe Social-Media-Slogans wie „Tod dem Datenschutz“ machen deutlich, dass Datenschutz immer noch als Bremsklotz betrachtet und Datenschutzbeauftragte als Verhindernde tituliert werden. „Das ist allerdings falsch“, macht Prof. Dr. Thomas Jäschke, Medizininformatiker und Professor für Wirtschaftsinformatik, klar.

> Ja, der DSB hat die Aufgabe zu kontrollieren. **Er hat aber vor allem auch die Aufgabe zu gestalten und zu beraten.**

Insofern sind Datenschutzbeauftragte auch Datenschutzberater:innen, die dabei helfen, die Projekte umzusetzen. Denn Lösungen sind vorhanden. Diese mögen Arbeit machen und Geld kosten, aber am Ende des Tages sprechen wir von einer wesentlichen Erhöhung der Sicherheit. Ich lade dazu ein, die ständigen Beschwerden über den Datenschutz einzustellen und stattdessen nach vorne zu blicken.

Der Blick nach vorne soll vor allem durch das Krankenhauszukunftsgesetz (KHZG) ermöglicht werden. Es stellt mit einem Fördervolumen von insgesamt 4,3 Milliarden Euro den größten Treiber dar, um den Digitalisierungsgrad zu erhöhen. Bei bewilligten Projekten müssen 15 Prozent der geförderten Summe für IT-Security und Informationssicherheit aufgewendet werden.

Bis die ersten Projekte aber messbare Erfolge erzielen, werden noch Jahre vergehen. Daher ist es keine Überraschung, dass das Bundesamt für Sicherheit und Informationstechnik (BSI) in seinem aktuellen Lagebericht von 2022 Alarm schlägt, dass die Gefährdungslage im Cyber-Raum so hoch war wie nie zuvor. Die digitale Erpressung durch Ransomware-Angriffe stelle dabei die größte Bedrohung dar. Zu demselben Ergebnis kommt auch die Sophos-Studie „State of Ransomware 2022“: Das Marktforschungsunternehmen Vanson Bourne befragte für den britischen Softwarehersteller weltweit 5.600 IT-Experten zur Ransomware-Entwicklung in insgesamt 31 Ländern. Darunter befanden sich 63 IT-Leitungen aus Deutschland in dem Bereich Gesundheitswesen.

Insgesamt hat sich innerhalb von 12 Monaten die Anzahl von Ransomware-Angriffen der befragten Unternehmen von einem Drittel (37 Prozent) auf fast zwei Drittel (66 Prozent) verdoppelt. Es lässt sich nicht leugnen: Hacker, die Organisationen durch Ransomware manipulieren, verbuchen einen hohen Erfolg, Tendenz steigend. Das liegt unter anderem daran, dass sie immer niederschwelliger kompetent sein müssen, um einen Angriff durchzuführen und gleichzeitig eine relativ hohe Bereitschaft von Unternehmen zugrunde liegt, Lösegeld zu zahlen. Immerhin waren es insgesamt 46 Prozent der Unternehmen im Jahr 2022, die sich erpressen ließen. Das Gesundheitswesen gehört zwar zu den Branchen mit der geringsten Bereitschaft, Lösegeld zu zahlen; der Grund, dass es über weniger Budget als andere Branchen verfügt, ist allerdings eher pragmatischer Natur.

Hoher Digitalisierungsgrad, hohes Risiko

Es darf klar und deutlich gesagt werden: Ein Cyberangriff auf eine Klinik setzt Menschenleben aufs Spiel. SensibleInformationen wie der Behandlungsablauf von Patient:innen oder die Funktionalität von OP-Geräten sind bei steigendem Digitalisierungsgrad einem erhöhten Risiko auf unbefugte Zugriffe ausgesetzt. Ob Trojaner-, Phishing- oder Ransomware-Angriffe: Es ist längst bekannt, dass menschliches Fehlverhalten die größte Sicherheitslücke von IT-Systemen ist. Die Verschlüsselung von Daten wird stetig komplexer - der Risikofaktor Mensch wird daher auch in Zukunft das größte Einfallstor für Hacker bleiben, sodass Angriffe niemals komplett ausgeschlossen werden können. Genau hier kommt das Business Continuity Managements ins Spiel. Die Managementmethode definiert alle Prozesse, um als Betrieb im Ernstfall handlungsfähig zu bleiben.

Insbesondere in Kliniken sollte der Schutz von Informationen – also die Informationssicherheit – Priorität haben, vor allem, wenn es um die IT-Sicherheit vor Cyberangriffen geht. Einmal mehr gilt es, Informationssicherheit und Datenschutz von Beginn an mit einzubeziehen. „Gesetzliche Anforderungen wie Security und Privacy by Design sind in Digitalisierungsprojekten frühzeitig zu berücksichtigen“, erläutert Thomas Jäschke, „im Bereich der Informationssicherheit wird im Sinne des Business Continuity Managements das Fundament für erfolgreiche Digitalisierungsprojekte geschaffen. Sie sind essenziell für die erfolgreiche und sichere Digitalisierung.“ Das Vorgehen, das von Anfang an umgesetzt werden muss, ist das sogenannte Security Engineering.

Experten identifizieren die Informationen und Daten in den vorliegenden Prozessen eines Digitalisierungsprojektes, indem sie eine Schutzbedarfsanalyse durchführen. Sie überprüfen dabei Prozesse und Assets hinsichtlich der drei primären Schutzziele „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“.

Der Schutzbedarfsanalyse folgen die Gefährdungs- und Risikoanalyse, in denen besonders gefährdete Assets und Prozesse betrachtet werden. Mithilfe einer Risikoanalyse werden entsprechende Maßnahmen abgeleitet, die das Weiterführen des Betriebs trotz Notfallsituation gewährleisten.

Tipp: Lesen Sie mehr über die Schutzbedarfs,-Gefährdungs- und Risikoanalyse im nachfolgenden Artikel ab Seite 8.

Unternehmen müssen Risiken einkalkulieren und bis zu einem gewissen Maße akzeptieren, auch das ist Teil von Business Continuity Management. Notfallkonzepte dienen dann als weiterführende Maßnahme für den Fall der Fälle. „Es gibt keinen Standardplan für Business Continuity Management. Die Maßnahmen müssen individuell für jede Organisation entwickelt werden. Was aber übergreifend für alle gilt, ist die Gründung eines Incident Response Teams, das im Notfall kontaktiert wird, klar definierte Ablauf- und Notfallpläne und nicht zuletzt die Sensibilisierung des gesamten Personals“, fasst Thomas Jäschke zusammen.

In einem Krankenhaus öffnen nicht nur IT-Mitarbeitende eine E-Mail, sondern vom Pförtner über die Verwaltung bis zum Klinikdirektor auch alle anderen Mitarbeitenden und schließlich auch externe Leistungserbringer:innen. Damit besteht in jeder Abteilung und in jeder einzelnen E-Mail die potenzielle Gefahr, eine Klinik zu gefährden. Entgegenwirken kann dem ein präventives Vorgehen durch entsprechende Awarenessmaßnahmen. Als Digitalisierungsexperte mit 30-jähriger Erfahrung weiß Thomas Jäschke, dass davon alle Seiten profitieren: „Wenn Unternehmen in die Sicherheit durch qualifiziertes Personal investieren und die Security-Awareness bei Mitarbeitenden erhöhen, dann ist das für sie bei ihren Anwendungen auch im privaten Umfeld ein Wissensgewinn. Wer eine Phishing-Mail erkennt und um ihre Folgen weiß, wird sie erst recht nicht auf dem eigenen Rechner zu Hause öffnen. Der Nutzen für den Einzelnen wird schnell begreifbar und das wirkt sich wiederum positiv auf das Unternehmen aus.“

Digitalisierungsprojekte müssen holistisch gesteuert werden

Während auf der einen Seite die zunehmende Digitalisierung in der Medizin die Angriffsfläche für Cyberkriminalität vergrößert und Informationen einer immer höheren Gefährdung durch Cyberattacken ausgesetzt sind, ist auf der anderen Seite die Bereitschaft für Investitionen in Cyber-Security, Informationssicherheit und Datenschutz überaus gering. So liegen IT-Budgets im Gesundheitswesen für Sicherheitsvorkehrungen im Schnitt bei nur 10 Prozent. Gibt es hier ein Effizienz-Problem?

„Ja“, meint Thomas Jäschke, „die größte Herausforderung im Digitalisierungsprozess für Kliniken ist der akute Personalmangel, insbesondere in der Digitalisierung und der IT. Krankenhäuser kommen nicht drumherum, mit externen Partner:innen zusammenzuarbeiten, die auf den Punkt das Know-how liefern, das bei der Umsetzung der digitalen Transformation benötigt wird. Folglich müssen interne Mitarbeitende dazu befähigt werden, externe Ressourcen zu steuern und ein vernünftiges Multiprojektmanagement voranzutreiben.“

Die Sensibilisierung der Mitarbeitenden durch entsprechende Schulungen und die Investition in qualifiziertes Personal verdeutlichen, dass Informationssicherheit ein Thema für die Managementebene ist und von hier aus in den Betrieb getragen werden muss. Magnus Welz, Bereichsvorstand IT- und Wissensmanagement der DATATREE AG, spricht aus Erfahrung, denn er setzt seit 15 Jahren Informationssicherheits- und IT-Projekte mit Kund:innen um: „Das Bereitstellen und die Ernennung von Verantwortlichen ist ein wichtiger Aspekt bei der Umsetzung von Digitalisierungsprojekten. Es geht hierbei um ganzheitliche Prozessbetrachtung: Ein Chief Digital Officer (CDO) hat eine klar benannte Stelle inne, die offiziell die Verantwortung für den gesamten Digitalisierungsprozess übernimmt – und das ist wichtig. In vielen Kliniken ist es noch immer so, dass die IT-Abteilung als Treiber der Digitalisierung verstanden wird. Bei gleichzeitigem Ressourcenmangel ist den Mitarbeitenden aber meistens gar nicht möglich, die Projekte auch strategisch voranzutreiben. Die IT ist und bleibt essenziell für die Umsetzung von Digitalisierungsprojekten. Ihre Steuerung jedoch muss holistischer gestaltet werden.“

> **Die Sicherheit von Digitalisierungsprojekten beginnt immer vor dem Angriff.**

„Informationssicherheit und Datenschutz im Rahmen des Business Continuity Managements zu spät oder sogar gar nicht mit einzubeziehen ist wie Autofahren ohne Sicherheitsgurt oder wie Motorradfahren ohne Helm“, zieht Thomas Jäschke das Fazit, „das würde heutzutage schließlich auch niemand mehr machen. Wenn alle Akteure im Projekt nicht endlich beginnen, miteinander in den Dialog zu treten und im Vorfeld präventiv für geeignete Sicherheitsstrukturen durch Business Continuity Management zu sorgen, dann werden wir immer wieder Schlagzeilen über digitale Erpressung lesen – und dass das am Ende für Kliniken erst recht teuer und für Patient:innen lebensgefährlich wird, sollte allen klar sein.“

Literatur

https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/221025_Lagebericht.html

https://assets.sophos.com/X24WTUEQ/at/43hhrb4tjnjg8jj9fmjq6s/sophos-state-of-ransomware-2022-wpde.pdf

Wer macht was, wann und warum?

Höhere Gewalt wie Naturkatastrophen, menschliche Eingriffe von außen in Form von Cyberangriffen oder von innen, beispielsweise durch Spionage oder Sabotage von Mitarbeitenden – all das gefährdet Organisationen und kann zu erheblichem Schaden führen. In einer Krisensituation greifen im besten Fall die im Rahmen des Business Continuity Managements festgelegten Strategien und Maßnahmen.

Text: Alexander Vogel

Aber wie viel Schutz braucht ein Unternehmen, welche Geschäftsprozesse sind besonders gefährdet und welche sollten in einer Notsituation als Erstes geschützt werden? Und mehr noch: Was bedeutet eigentlich „geschützt“ und wie werden relevante Prozesse und Assets schnellstmöglich wieder funktionstüchtig?

Um Fragen wie diese nicht willkürlich aus dem Bauch heraus zu beantworten, setzen sich Experten mit der Organisation und ihren Produktionsstätten auseinander. Sie analysieren, welche Prozesse und welche Assets kritisch für das Unternehmen sind und welchen Risiken diese ausgesetzt sind.

Für die Wahrung der Schutzziele der Informationssicherheit werden innerhalb einer Schutzbedarfsanalyse sowie der anschließenden Gefährdungs- und Risikoanalyse ermittelt, was die unternehmenskritischen und -wichtigen Prozesse und Assets sind und welchen Gefährdungen und Risiken diese unterliegen. Darauf aufbauend werden Prozesse zur Organisation im Krisenfall entwickelt.

Über den Autor Alexander Vogel

Alexander Vogel ist Senior Berater für den Bereich Datenschutz und seit über zehn Jahren für die DATATREE AG tätig. Seine Schwerpunkte umfassen die Projektleitung in den Bereichen der medizinischen Informationssysteme sowie Datenschutzprojekte von Großkunden im Gesundheitswesen.

DIE SCHUTZBEDARFSANALYSE

Die Schutzbedarfsanalyse ist der Start für Informationssicherheitsbeauftragte, um herauszufinden, welche Prozesse in einer Organisation Schutz benötigen und wie hoch ihr Schutzbedarf jeweils sein sollte. Sie ist die Grundvoraussetzung für die darauffolgende Gefährdungs- und Risikoanalyse.

DIE HERANGEHENSWEISE: TOP-DOWN VS. BOTTOM-UP

Grundsätzlich gibt es zwei unterschiedliche Herangehensweisen, die in ihren Wirkungsrichtungen unterschiedlich sind: Top-Down oder Bottom-Up. Gehen Experten „von unten nach oben“ - also Bottom-Up, nehmen sie zunächst kleinste Assets unter die Lupe, wie beispielsweise den Laptop mit der Inventarnummer 4711, und arbeiten sich dann in höhere Hierarchien vor, bis sie zum Beispiel im Prozess der Befundung einer CT-Untersuchung angelangt sind. Voraussetzend und gleichzeitig nachteilig für dieses Vorgehen ist, dass im Vorfeld eine Liste mit allen Assets vorhanden sein muss. Die Erstellung ist oft mühsam, zeit- und ressourcenaufwendig.

Der Top-Down-Ansatz geht genau umgekehrt vor: Experten beginnen auf Prozessebene, also einem übergeordneten Ziel und arbeiten sich dann weiter nach unten zu einzelnen Assets vor. Dies birgt die Vorteile, dass ein Assetmanagement nach und nach aufgebaut werden und das Risikomanagement in Form der Schutzbedarfsanalyse zeitnah starten kann. Ebenfalls führt der Top-Down-Ansatz zu einer prozessorientierten Risikobetrachtung.

WAS HEISST EIGENTLICH „SCHUTZ“?

Das Ziel, ein Unternehmen zu schützen, klingt erst einmal einleuchtend. Was genau aber muss und kann geschützt werden? Genauer betrachtet ist der Begriff “Schutz” sehr abstrakt, nicht eindeutig definierbar und schon gar nicht ganzheitlich überprüfbar. Und um es noch komplizierter zu machen: Was tatsächlich geschützt werden muss, ist organisationsabhängig. Für wirtschaftsorientierte Unternehmen sind insbesondere finanzielle Auswirkungen existenziell, hier ist besonders der Schutz von Assets oder Prozessen relevant, bei denen im Schadensfall hohe Kosten entstehen. Für Behörden hingegen ist häufig die Reputation von hoher Bedeutung und schützenswert, damit sie möglichst nicht angekratzt wird. One size fits all - in der Schutzbedarfsdefinition gibt es das nicht.

Um den tatsächlichen Schutz besser einordnen zu können und greifbar zu machen, wurden Schutzziele definiert, die einzelne Einheiten in einer Organisation eingrenzen. In der Informationssicherheit stehen besonders drei Schutzziele im Fokus: Vertraulichkeit, Integrität und Verfügbarkeit. Je nach Anforderung gibt es weitere Schutzziele, wie beispielsweise Authentizität, Zurechenbarkeit oder Verbindlichkeit. Im Gesundheitswesen werden auch Schutzziele wie Patientensicherheit und Behandlungseffektivität definiert. Die Entscheidung, welche Schutzziele innerhalb der Schutzbedarfsanalyse herangezogen werden, ist wiederum von der Organisationsstruktur abhängig und wird je nach Bedarf entschieden.

Die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit gelten allerdings als Grundwerte und sollten innerhalb der Schutzbedarfsanalyse immer abgedeckt sein.

VERTRAULICHKEIT

Es ist so naheliegend wie relevant: Nur befugte Personen dürfen vertrauliche Informationen einsehen, bearbeiten und verwalten. Unter dem Schutzziel der Vertraulichkeit wird von Informationssicherheitsexperten entsprechend überprüft und festgelegt, wer welche Informationen einsehen und bearbeiten darf und welche Maßnahmen - beispielsweise Verschlüsselung - getroffen werden müssen, damit Unbefugte keinen Zugriff haben.

INTEGRITÄT

Informationen müssen verlässlich sein und bleiben. Unter dem Schutzziel der Integrität fallen daher alle Maßnahmen, die dazu beitragen, die Unversehrtheit von Daten sicherzustellen. Werden Informationen verändert, ist es wichtig, die Änderungen nachvollziehen zu können.

VERFÜGBARKEIT

Das Schutzziel Verfügbarkeit bezieht sich auf die gesamte Dauer, in der die Systeme im Unternehmen funktionieren, also verfügbar sind. Im Rahmen der Risikoanalyse wird unter diesem Schutzziel erörtert, welche Systeme oder Daten verfügbar sein müssen, damit das Unternehmen trotz Krisenfall im Betrieb bleibt.

Sind die Schutzziele definiert, beschäftigen sich Experten mit der Frage: Wie hoch ist der Schutzbedarf? Das Bundesamt für Sicherheit und Informationstechnik (BSI) empfiehlt deshalb drei Schutzbedarfskategorien, die einen potenziellen Schaden zunächst folgendermaßen einordnen:

NORMAL	Die Schadensauswirkungen sind begrenzt und überschaubar.
HOCH	Die Schadensauswirkungen können beträchtlich sein.
SEHR HOCH	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.[1]

[1] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_4_Schutzbedarfsfeststellung/Lektion_4_01/Lektion_4_01_node.html

Wann ein Asset oder ein Prozess einen normalen, hohen oder sehr hohen Schutzbedarf hat, ist auch hier wieder von der Organisation abhängig und muss individuell betrachtet werden: Während ein finanzieller Schaden von bis zu 100.000 Euro für einen Großkonzern überschaubar sein kann, ist er für ein mittelständisches Unternehmen unter Umständen existenzbedrohend. Informationssicherheitsexperten müssen also auch hier von Fall zu Fall abwägen, welche Schutzbedarfskategorie zutrifft. Die Schutzbedarfsanalyse ist abgeschlossen, wenn alle zu bewertenden Assets und Prozesse auf die definierten Schutzziele hin überprüft und bewertet wurden.

DIE GEFÄHRDUNGS- UND RISIKOANALYSE:

Die Gefährdungs- und Risikoanalyse beginnt zunächst mit der Betrachtung derjenigen Prozesse oder Assets, die in der vorangegangenen Schutzbedarfsanalyse in die Kategorie „sehr hoch“ gefallen sind. In einem späteren Schritt folgt auch die Betrachtung der mit „hoch“ bewerteten Prozesse oder Assets.

Das BSI empfiehlt die Erstellung eines Gefährdungskatalogs. In diesem werden zunächst Szenarien kreiert, um zu betrachten, welche Prozesse bzw. Assets einer Gefährdung ausgesetzt sind. Stehen beispielsweise die Server eines Krankenhauses im Keller und liegt das Krankenhaus in der Nähe eines Flusses, wird das Szenario „Hochwasserkatastrophe durch Starkregen“ betrachtet. Jedem Szenario wird somit eine eigene Risikogefährdung zugeordnet. Im genannten Beispiel ist die Risikogefährdung hoch. Läge das Krankenhaus fern von Wasser, wäre die Gefährdung entsprechend niedrig. Auf diese Weise kann dann die Eintrittswahrscheinlichkeit für das potenzielle Risiko bewertet werden, mit der die Gefährdung tatsächlich eintritt.

In der hieraus resultierenden Risikobehandlung wird schließlich die Frage beantwortet: Was soll im Falle einer Gefährdung passieren?

Die Risikobehandlung wird in der Regel
in folgende Klassen unterteilt:
• AKZEPTANZ • MINDERUNG • ÜBERTRAGUNG • VERMEIDUNG

Denn hierauf kommt es schließlich an: Kann und muss das Risiko im Vorfeld vermieden werden? Ist das Risiko so hoch, dass es reduziert werden muss – und wenn ja, wie? Oder kann ein Risiko sogar akzeptiert werden? Wird beispielsweise dem Geschäftsprozess „Server Betrieb“ der Verlust von Hardware mit dem Risiko „mittel“ bewertet, so fällt die Entscheidung hier möglicherweise auf „Risikoakzeptanz“ und es müssen keine Ressourcen in Maßnahmen fließen, um das Risiko auszuschließen. Für die Akzeptanz gibt es wiederum „Risikoakzeptanzkriterien“, die für jede Organisation individuell ausfallen und im Vorfeld bestimmt werden. Fällt beim Geschäftsprozess „IT-Wartung“ das Szenario „Personalausfall“ in die Risikogruppe der Kategorie „sehr hoch“, so wird die darauffolgende Entscheidung „Risikominderung“ entsprechende Strategien - beispielsweise Personalaufbau - erfordern, um dieses Risiko auf minimalem Niveau zu halten. Die vorgeschlagenen Maßnahmen werden dabei genau dokumentiert, ebenso wie das immer verbleibende Restrisiko.

Eine Risikoanalyse ist nicht in Stein gemeißelt und so wandelbar wie der Alltag in einer Organisation. Wenn neue Technologien in der Lage dazu sind, Cyberangriffe aggressiver in IT-Systeme eindringen zu lassen, nimmt das damit verbundene Risiko zu und der Schaden wird womöglich größer. Aus diesem Grund ist sie immer in einem gewissen Zyklus zu wiederholen und Prozesse und Assets sind immer wieder neu zu bewerten. Im Gesundheitswesen beispielsweise werden Gefährdungs- und Risikoanalysen jährlich wiederholt.

Fazit

Wer seine Organisation schützen möchte, sollte auf Prophylaxe statt auf Therapie setzen.

Die im Vorfeld durchgeführten Schutzbedarfs- sowie Gefährdungs- und Risikoanalysen kategorisieren ein Unternehmen in sinnvolle Einheiten und machen willkürliche und teilweise überteuerte Vorsorgemaßnahmen obsolet. Gleichzeitig schützen sie die Organisation kalkuliert und nachhaltig. Dabei hat jede Organisation individuelle Schwerpunkte und Schwachstellen und damit auch individuelle Risikoeigenschaften. Es gibt keine Einheitsmaßnahmen, deshalb lohnt es sich Experten zu engagieren, die mit einem geschulten Auge eine Organisation individuell auf ihre Risiken hin bewertet.

Möchten Sie wissen, wie gut Ihr Unternehmen im Krisenfall geschützt ist und was Sie optimieren können?

Die Informationssicherheitsexperten der DATATREE AG unterstützen Sie dabei. Wenden Sie sich hierzu gerne an: sales@datatree.ag

INFORMATIONSSICHERHEIT IM KRANKENHAUS: Gestern, Heute und in Zukunft

Ein Interview mit Mike Zimmermann

Mike Zimmermann ist Informationssicherheitsbeauftragter im Universitätsklinikum Carl Gustav Carus in Dresden. Die Klinik ist seit 1999 eine Anstalt des öffentlichen Rechts des Freistaates Sachsen und gehört zu den größten führenden Kliniken in Deutschland. In unserem Exper*Site*-Interview berichtet er über die Herausforderungen der Digitalisierung im Gesundheitswesen, über die Veränderung seiner Position mit steigenden Sicherheitsanforderungen und wie er sich die Zukunft der Informationssicherheit im Gesundheitswesen vorstellt.

ExperSite *Herr Zimmermann, Sie sind seit 11 Jahren als Informationssicherheitsbeauftragter im Universitätsklinikum Carl Gustav Carus Dresden beschäftigt. Können Sie zusammenfassen, wie sich Ihre Position seitdem verändert hat? Vor welchen Herausforderungen standen Sie damals? Vor welchen Herausforderungen stehen Sie heute?*

Mike Zimmermann: Anfangs war ich noch mit dem Aufbau der operativen IT-Sicherheit beschäftigt. Natürlich hatten wir damals schon Firewalls oder Endpoint Protection Systeme im Einsatz, aber die Aufgabe bestand darin, die Klinik-Administratoren durch Zentralisierung und Standardisierung dieser sicherheitsrelevanten Systeme zu entlasten. In dieser Zeit war das Verständnis für IT-Sicherheit noch extrem gering und wurde eher als etwas Negatives empfunden, da zum Beispiel die Virenscanner im Verhältnis noch sehr viel Prozessorlast der IT-Systeme in Anspruch nahmen oder beim wöchentlichen Vollscann der Systeme nahezu nichts anderes mehr mit dem System gemacht werden konnte. Ich erinnere mich an viele Diskussionen mit den Anwendern und IT-Administratoren.

Mit den ersten Erkenntnissen zum damals neuen IT-Sicherheitsgesetz wurde ich dann zum ISB ernannt, klassischerweise nicht mehr in der IT angesiedelt, sondern direkt dem Vorstand unterstellt. Die Aufgaben wechselten sukzessive immer mehr von der operativen hin zu der strategischen IT-Sicherheit. Anfangs bestand die Herausforderung darin, das Verständnis, aber auch die Verantwortung für IT-Sicherheit in den Klinik- und Geschäftsbereichsleitungen zu etablieren. Es war nicht einfach, zumal es damals kaum öffentlich bekannte Angriffe gab und die wenigen Veröffentlichungen entweder sehr weit entfernt waren oder in der Regel kaum unsere Branche betrafen.

Ein wichtiges Merkmal meiner Arbeit heute besteht darin, nicht irgendwelche Verbote zu definieren, sondern ich versuche auch immer zu verstehen, warum Prozesse oder Praktiken so umgesetzt werden. Meiner Meinung nach fördern wir mit reinen Verboten nur die Kreativität der Benutzer:innen, um neue, andere, meistens nicht weniger gefährliche Wege zu finden, um ihre Arbeitsprozesse zu optimieren. Ich kann sie oftmals verstehen und im Dialog versuchen wir den schmalen Pfad zwischen Usability und IT-Sicherheit zu finden.

> Wir können nur gemeinsam die aktuellen Herausforderungen meistern

> Ein wichtiges Merkmal meiner Arbeit besteht darin zu verstehen, anstatt Verbote zu definieren.
>
> MIKE ZIMMERMANN
>
> *Informationssicherheitsbeauftragter im Universitätsklinikum Carl Gustav Carus in Dresden*

Aktuell gibt es für alle Krankenhäuser eine riesengroße finanzielle Herausforderungen aufgrund der Pandemie und dem Krieg in der Ukraine und den damit verbundenen teilweise enorm gestiegenen Beschaffungs- und Verbrauchskosten wie beispielsweise Energie. Ein wichtiges Credo unserer Universitätsklinik besteht darin, Prozesse nicht nur in unserem Hause zu formen, sondern auch in und vor allem für die Branche aktiv die Vorgaben mit zu definieren. Ein Beispiel sind die gemeinsamen Ausarbeitungen der ersten Handlungsempfehlungen für Krankenhäuser zum Aufbau von IT-Sicherheit im Rahmen des UP-KRITIS Branchenarbeitskreises „Medizinische Versorgung“. Heute bin ich in vielen externen Arbeitskreisen tätig und versuche nicht nur mitzugestalten, sondern vor allem auch die gemeinsame Bewältigung von Themen zu forcieren. Was somit einem weiteren wichtigen Credo unseres Hauses entspricht, dass wir gerne unsere Erfahrungen teilen wollen, um uns letztendlich gegenseitig in Bereichen zu helfen, in denen wir aus meiner Sicht mittelfristig nur gemeinsam erfolgreich die Herausforderungen bewältigen können!

ExperSite *Im Jahr 2015 ist das IT-Sicherheitsgesetz 2.0 (IT-SiG) in Kraft getreten. Im Jahr 2017 kam dann die KRITIS-Verordnung nach dem BSI-Gesetz (BSI-KritisV), durch die Ihr Haus als kritische Infrastruktur definiert wurde. Wie haben diese gesetzlichen Regelungen Ihre Tätigkeit als ISB verändert?* >>>

Mike Zimmermann: Grundsätzlich haben die gesetzlichen Regulierungen einen sinnvollen Rahmen definiert. Ehrlich gesagt spart es auch viel interne Diskussionszeit, wenn ich auf Gesetze und Verordnungen verweisen kann und nicht argumentieren muss, ob denn nur wir Lösungen für Probleme suchen müssen. Ich würde mir aber wünschen, dass wir oftmals etwas mehr Zeit zwischen Gesetzes- bzw. Verordnungserlass und der Umsetzungsfrist hätten. Ein weiterer wichtiger Wunsch ist, dass der Gesetzgeber vor allem im Gesundheitssektor mit jeder Regulierung auch gleich die Finanzierung bestimmt. Es soll jetzt aber nicht der Eindruck entstehen, dass wir ohne Finanzierung keine IT-Sicherheitsmaßnahme durchsetzen wollen, aber wir müssen bei der besonderen Abrechnungsmethodik für Krankenhäuser immer wieder um jeden Euro kämpfen. Ich möchte auch gerne anregen, dass wir gelebte bzw. praktizierte Informationssicherheit fördern müssen, was sich zum Beispiel mit der Ermittlung eines Reifegrades und damit verbundenen Finanzierungstufen mittlerweile gut abbilden ließe. Sprich: Krankenhäuser erhalten je nach erreichtem Reifegrad Zulagen für die Finanzierung der IT-Sicherheit.

Insgesamt sind manche Anforderungen weniger verständlich und einzeln betrachtet sogar sinnlos, aber wie mittlerweile in allen Bereichen des Lebens, gibt es für die wenigsten Fragen nur noch ein einfaches Ja oder Nein. Die Komplexität wird immer weiter zunehmen und so müssen wir auch die Informationssicherheit ganzheitlich betrachten.

> Wir müssen gelebte Informationssicherheit in Krankenhäusern fördern

ExperSite *Schließlich wurde 2020 das Krankenhauszukunftsgesetz (KHZG) erlassen, das Krankenhäuser in die Lage versetzen soll, in moderne Notfallkapazitäten, die Digitalisierung und in IT-Sicherheit investieren zu können. Wie schätzen Sie den Erfolg des KHZG ein, wo sehen Sie Optimierungsbedarf?*

Mike Zimmermann: Das KHZG hat ursprünglich eine sehr gute Idee verfolgt und wir beschweren uns manchmal auf einem hohen Niveau. Es ist meines Erachtens das erste Förderprogramm, bei dem man nicht nur Investitionen abrechnen kann, sondern auch Dienstleistungen, Beratungen und vor allem auch Personalkosten für einen bestimmten Zeitraum. Die Gesamtfördersumme klingt erst einmal viel, aber geteilt durch alle Krankenhäuser und deren Digitalisierungs- und IT-Sicherheitsprojekte bleibt dann doch nicht mehr so viel übrig und wir haben sehr viel Nachholbedarf bei diesen beiden Themen in unserer Branche! Aber wie gesagt: 1 Million Euro sind besser als 0 Euro.

Kritisch sehe ich aber in der Tat zwei Probleme:
Zum einen wird es durch diesen enormen Investitionsschub für die Branche zunehmend schwieriger werden, Ressourcen zu finden, mit denen man diese Projekte zeitgerecht umsetzen kann, woran letztendlich die Qualität leiden wird.

Und zum anderen sehe ich wie bei allen Förderungen das Problem: Wie geht's weiter, nachdem die Gelder geflossen sind? In drei, spätestens fünf Jahren müssen erste Ersatzinvestitionen getätigt werden, oder wie sonst kann das jetzt finanzierte und qualitativ notwendige Personal gehalten werden? Vermutlich nicht nur die kleineren Häuser benötigen weitere Förderungen, um die Digitalisierungs- und Informationssicherheitsthemen auch dann noch weiter betreiben zu können.

> Das KHZG ist grundsätzlich eine sehr gute Idee. Aber wie geht es nach der Förderung weiter?

ExperSite *Unter anderem die Resilienz der IT-Systeme in KH steht immer wieder im Fokus, wenn es um zunehmende Digitalisierungsmaßnahmen geht. Wie setzen Sie das im Universitätsklinikum Carl Gustav Carus Dresden um?*

Mike Zimmermann: Zuallererst muss der Stellenwert der IT angepasst werden. Wenn ich Benutzer:innen dahingehend befrage, wird die IT immer noch häufig auf E-Mails und Internet beschränkt. Die jetzt schon vorhandene sehr hohe digitale Abhängigkeit wird vielen dann erst im weiteren Gesprächsverlauf bewusst.

Zusätzlich zeichnen sich unsere angebotenen IT-Services bisher durch eine sehr hohe Verfügbarkeit aus. Das führt zu der Erwartung, dass die IT oder auch die vernetzte Medizintechnik nicht ausfallen wird. Prinzipiell super, aber die Sensibilisierung hinsichtlich der Business Continuity bei Ausfall digitaler Prozesse steht dadurch natürlich nicht an erster Stelle.

Die IT ist sich der Wichtigkeit der IT-Resilienz bewusst, aber durch die Ressourcenknappheit in allen Belangen kann dies oftmals nicht vollumfänglich bewertet werden und steht somit unter enormen Druck. Es muss aber letztendlich jedem Klinik-Prozessverantwortlichen bewusst sein, dass auch dies in seiner Verantwortung steht.

> Die sehr hohe digitale Abhängigkeit ist vielen Benutzer:innen gar nicht bewusst

ExperSite *Immer wieder liest man auch von unklaren Verantwortlichkeiten, fehlenden personellen Ressourcen, einem mangelnden Verständnis für die Ernsthaftigkeit des Themas oder sogar der IT selbst, wenn es um Digitalisierungsmaßnahmen im Gesundheitswesen geht. Können Sie das bestätigen? Und wo erleben sie Schwachstellen und weiteren Handlungsbedarf?*

Mike Zimmermann: Die fehlenden Ressourcen und das damit verbundene fehlende Know-how ist aus meiner Sicht derzeit die größte Herausforderung bei der Digitalisierung. Oftmals werden analoge Prozesse eins zu eins digitalisiert, ohne dass eine umfassende Prozessprüfung stattfindet. Richtig frustrierend wird es dann für die Benutzer:innen, wenn es schon schlechte analoge Prozesse waren. Wichtig wie bei allen Prozessänderungen ist, dass wir die Benutzer:innen mitnehmen und auf ihre Bedarfe eingehen oder anders ausgedrückt: Die IT und die Informationssicherheit müssen begleiten, aber nicht die Prozesse federführend definieren.

> Das fehlende Know-how ist die größte Herausforderung in der Digitalisierung

ExperSite *Grundsätzlich geht es beim Business Continuity Management darum, die Aufrechterhaltung des Geschäftsbetriebes auch bei einer Störung sicherzustellen. Welche Prozesse mit welchen Maßnahmen stoßen Sie im Falle eines Cyberangriffs im UKDD an, um die Informationssicherheit weiterhin gewährleisten zu können?*

Mike Zimmermann: Wir haben als Krankenhaus viel Erfahrung mit Ausnahmesituationen wie Hochwasser oder der Versorgung von vielen Verletzten zur gleichen Zeit. Cyberangriffe waren vor Neuss und Düsseldorf noch so weit weg bzw. sehr abstrakt, aber spätestens seit dem Vorfall am UK Düsseldorf sind sich alle Verantwortlichen der möglichen Konsequenzen eines Informationssicherheitsvorfalles bewusst. Der vorhandene klinikumsweite Alarm- und Einsatzplan wurde angepasst und es wurden Strukturen geschaffen, die unter anderem durch die Erkenntnisse und Erfahrungen aus Düsseldorf entwickelt wurden. Zum Beispiel wurde das Lagezentrum für IT-Notfälle erweitert, sodass die IT integriert werden kann, inklusive mögliche externe IT-Unterstützung. Bei der Analyse eines möglichen IT-Totalausfalls an unserem Klinikum wurden mögliche Schwachstellen identifiziert und werden nun priorisiert bearbeitet. In der IT gibt es verschiedene Projekte zu Themen wie der Kommunikation im Notfall, dem Wiederanlauf oder auch der Forensik. Auch das regelmäßige Üben ist Bestandteil dieser Notfallkonzepte.

In den jeweiligen Kliniken und Geschäftsbereichen werden Notfallkonzepte entwickelt, um die Geschäftsfortführung der kritischen Dienstleistungen sicherzustellen. All diese Anforderungen kommen zusätzlich auf die betroffenen Bereiche dazu. Die Notwendigkeit ist allen bewusst, aber auch hier muss aufgrund der vorhandenen Ressourcen priorisiert werden. Für mich ist wichtig - wie bei allen anderen Informationssicherheitsthemen: Wir müssen uns stetig weiterentwickeln und besser werden.

ExperSite *Häufig merken wir bei DATATREE AG, dass die Sensibilisierung aller Mitarbeitenden ein wichtiger Bestandteil ist, um die Informationssicherheit in eine Organisation nachhaltig zu implementieren. „Die größte Schwachstelle in der IT ist der Mensch" ist ein Satz, der in diesem Zusammenhang gerne fällt, wenn es um IT-Security in Organisationen geht. Teilen Sie diese Meinung?*

Mike Zimmermann: Ja, selbstverständlich ist der Mensch die größte Schwachstelle.

Wir machen Fehler, was auch wichtig ist, um daraus zu lernen und uns weiterzuentwickeln. Leider sehe ich aber oftmals die falsche Fehlerkultur und man stürzt sich nach Vorfällen lieber auf den vermeintlichen Verursacher und kennt keine Gnade mit Vorwürfen, anstatt konstruktiv nach Lösungen zu suchen!

Oftmals werden uns nicht ausreichend Ressourcen zur Verfügung gestellt. Das Lernen und Ausprobieren sind sehr wichtig, um beispielsweise sichere Anwendungen zu entwickeln oder fit im Umgang mit der IT zu sein. Wir Menschen reagieren emotional und haben Ängste, die zu Reaktionen führen, die wir zu anderen Zeitpunkten so nicht getätigt hätten. Diese Eigenschaften werden ausgenutzt - im Positiven wie im Negativen! Auch für mich ist Sensibilisierung ein wichtiger Baustein in der Informationssicherheit. Die bisherige klassische regelmäßige Massen-„Grundbetankung“ der Benutzer:innen ist aber nicht sinnvoll. Wir müssen Awareness-Kampagnen erarbeiten, in denen zwar eLearning enthalten ist, aber durch viele anderen Medienformate und Inhalte ergänzt werden. Wir haben unterschiedliche Zielgruppen mit diversen Reifegraden. Der eine mag lieber eine spielende Vermittlung mit Gamification und andere lesen lieber einfache textbasierte Inhalte auf der Heimfahrt im Zug. Die Erfahrungen zeigen, dass Sensibilisierungen schnell wieder in Vergessenheit geraten oder gar schon bei der Schulung gelangweilt/genervt vom Thema sind. Gerade letztere Gruppe sind aus meiner Sicht auch die potenziell anfälligsten Benutzer:innen.

Es ist eine enorme Herausforderung und vor allem eine permanente Aufgabe User Awareness zu schaffen und nachhaltig zu etablieren! Wir müssen auch hier mit Emotionen arbeiten, natürlich nicht um Angst und Schrecken zu verbreiten, wie es Angreifer:innen tun, sondern im positiven Sinne. Erschwerend kommt noch dazu, dass Informationssicherheit im Krankenhaus nur ein kleiner Teil von vielen verpflichtenden Schulungen der Mitarbeitenden ist. Zusammengefasst bedeutet das: Sensibilisierung ist wichtig, als eine von vielen technischen und organisatorischen Bausteinen in der Informationssicherheit!

> Oft wird sich nach Vorfällen auf den/die vermeintlichen Verursachenden gestürzt, anstatt konstruktiv nach Lösungen zu suchen.

Exper*Site* *Ein Blick in die Zukunft aus Sicht eines Experten: An welcher Stelle steht Informationssicherheit in 10 Jahren? Welche Veränderungen / Trends erwarten und erhoffen Sie in Bezug auf Informationssicherheit in kritischen Infrastrukturen?*

Mike Zimmermann: Die grundlegende Methodik wird sich nicht ändern, sprich, wir werden immer wieder am besten möglichst zeitnah auf neue Bedrohungen reagieren müssen und es wird nie eine 100% Sicherheit geben! Wie immer werden neue Technologien sowohl positive als auch negative Veränderungen mit sich bringen. KI ist ein aktuelles, gutes Beispiel, obwohl ich oftmals unterstelle, dass mit KI geworben wird, obwohl sie letztendlich noch nicht drinsteckt. Aber es pusht das Thema derzeit enorm. KI wird uns sehr viel Positives bringen, selbstverständlich werden andererseits Angreifer:innen die KI auch für ihre Use Cases einsetzen.

Viele der bisherigen Prozesse werden aus meiner Sicht einer großen Transformation unterliegen und somit viele Veränderungen und Anpassungsbedarf mit sich bringen. Bisherige Ansätze der onPrem Datenhaltung werden zumindest zu hybriden cloud-/onPrem-basierten Umsetzungen führen.
Wir sind auf dem Weg zu einer datenzentrierten Infrastruktur, was die Voraussetzung für das erforderliche Teilen und Verschieben unseres wichtigsten Assets, den Daten sein wird. Nicht nur um die Sicherheit (Verfügbarkeit und Zuverlässigkeit) zu erhöhen, sondern auch um neue und absolut notwendige Use Cases durch das Verknüpfen dieser Daten zu erhalten. Gerade im Medizinsektor wünsche ich mir dadurch unter anderem Heilungschancen, die bisher noch nicht möglich sind.

Letztendlich wird es wichtig sein, dass die Informationssicherheit und der Datenschutz immer ein Bestandteil aller Krankenhausprozesse sein muss! Und wie schon seit eh und je werden wir uns rückblickend fragen, wie zeitintensiv - da ohne Automatisierung und deshalb kompliziert - haben wir früher nur analysiert? Was aber nicht bedeutet, dass man im Jetzt und Hier mehr Zeit für angenehmere Dinge haben wird!

Wie erkenne ich Phishing-E-Mails und Phishing-Webseiten?

Phishing-E-Mails und Phishing-Webseiten verfolgen vor allem das Ziel, Usern sensible Daten zu entlocken. Die Angreifer:innen werden dabei immer professioneller. Wir verraten Ihnen, wie Sie gefälschte Webseiten und E-Mails trotzdem erkennen.

Text: Andreas Pillen

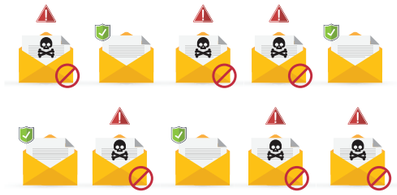
Was bedeutet Phishing?

Unter dem Begriff Phishing (Neologismus von fishing, engl. für "Angeln") versteht man Versuche, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdige:r Kommunikationspartner/in in einer elektronischen Kommunikation auszugeben. Ziel des Betrugs ist es, z. B. an persönliche Daten eines Internet-Benutzers zu gelangen, oder ihn zur Ausführung einer schädlichen Aktion zu bewegen.

Spam-Mails im Namen von Unternehmen

Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) betrug im Februar 2022 die Spam-Ratio 4,5. Das bedeutet, dass auf 100 legitime Mails eines Unternehmens zusätzlich 450 Spam-Mails durch Externe im Namen des Unternehmens entworfen wurden.

Das war im Betrachtungszeitraum Juni 2021 bis Mai 2022 ein Spitzenwert. Der Durchschnitt in diesem Zeitraum lag bei Faktor 2 und ist damit auch noch erschreckend hoch: demnach kamen auf 100 legitime Mails im Durchschnitt 200 Spam-Mails.



Der Anteil von Phishing-Mails am Gesamtaufkommen der Spam-Mails betrug rund 30%.

100 legitime Mails, 200 Spam-Mails -

das ergibt 60 Phishing-Mails pro 100 legitime Mails.

Es ist also keine Frage, ob Sie bzw. Ihr Unternehmen ein Opfer einer Phishing-Mail oder einer Phishing-Webseite sein werden oder nicht.

Es ist lediglich die Frage, wann und mit welchen Folgen!

Über den Autor Andreas Pillen:
Andreas Pillen ist Berater für Informationssicherheit und Datenschutz bei der DATATREE AG. Als Product-Owner für Phishing-Kampagnen sensibilisiert er Kund:innen durch Schulungen und speziell auf das Unternehmen ausgerichtete Kampagnen für den Schutz vor Phishing-Attacken.

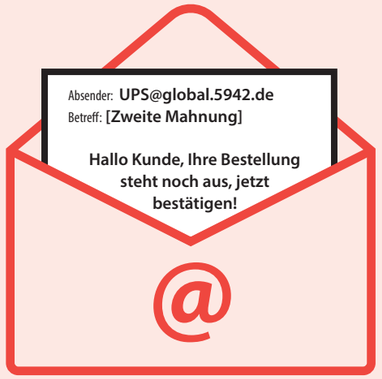
Literatur
BSI-Lagebericht 2022, Seite 26ff

Wie erkenne ich eine Phishing-Mail?

Nehmen wir als Beispiel eine Mail, die ich vor ein paar Tagen selbst erhalten habe. Hier war der vermeintliche Absender die Firma UPS.

Zu Beginn sollte unser **gesunder Menschenverstand** walten und wir dürfen uns fragen, warum wir diese E-Mail erhalten haben. – Wenn wir kein Paket über UPS versendet haben und auch keines erwarten, sollten wir bereits jetzt skeptisch hinsichtlich des Erhalts dieser Mail sein.

Der Absender der Adresse lautet: UPS@global.5942.de – Für E-Mails verwendet das Unternehmen aber die Domain ups.com, wie schnell im Internet nachvollziehbar ist. Warum sollte UPS über eine Domaine @global.5492.de schreiben? – Wer Zweifel hinsichtlich der Echtheit einer E-Mail hat, kann sich auch mit dem vermeintlichen Absender, hier also UPS, über einen anderen Weg, z. B. per Telefon in Verbindung setzen und nachfragen, ob eine solche Absenderadresse vom Unternehmen überhaupt benutzt wird.



Der **Betreff** der E-Mail lautet: „[Zweite Mahnung] Hallo Kunde, Ihre Bestellung steht noch aus, jetzt bestätigen!“ Hier wird ein dringender Handlungsbedarf suggeriert, gerade auch, wenn eine „Erste Mahnung“ wissentlich nicht besteht.

Bei einem Blick auf den **Text selbst** fällt sofort die unpersönliche Anrede „Hallo Kunde“ ins Auge, wie sie bereits im Betreff benutzt wurde. Weiterhin ist der Text inhaltlich verwirrend formuliert: Der gesamte Textfluss passt nicht zu einem weltweit agierenden Global Player, der für die Erstellung seiner Texte Marketing-Expert: innen engagiert.

Die Erklärung in diesem Fall:
Oftmals werden Phishing-Mails oder -Webseiten im Ausland erstellt und durch Übersetzungsprogramme in die jeweilige Landessprache übersetzt. Das Ergebnis sind folglich Formulierungen, die professionell agierenden Muttersprachlern nicht zugerechnet werden können.

Bei Betrachtung mittels „Mouseover“ des **Links** hinter dem Button „Vereinbaren Sie eine Zustellung“, kommt folgende **Ziel-URL** zum Vorschein: https://jlfhjlfhljfhlfhjmiptuip.page.link/Eit5jfgdghldgjldgjl

Auch dieser Link hat nichts mit einem Link der Firma UPS zu tun. Er ist ein eindeutiger Hinweis auf eine Phishing-Mail.

Klicken Sie auf gar keinen Fall auf diesen Link!

Haben Sie es doch getan, sind folgende Dinge zu erwarten:

- Start des Downloads von Schadsoftware (z. B. Ransomware) auf den eigenen Rechner sowie deren Ausführung;
- Weiterleitung auf eine gefälschte Webseite von „UPS“, auf der Informationen, wie Zugangsdaten oder Daten einer Bankverbindung, abgefragt werden;
- Aufforderung zum Download von weiterer Schadsoftware, die z. B. als vermeintliche

5 TIPPS, wie Sie eine Phishing-E-Mail erkennen

- Gefälschte Absender-Adresse
- Abfrage vertraulicher Daten
- Vorgetäuschter „dringender“ Handlungsbedarf
- Links zu gefälschten Webseiten

Wir nehmen Phishing-Webseiten für Sie unter die Lupe.

So gehen wir in unserem Webseiten-Test vor:

Im Rahmen einer besonders gesicherten Systemumgebung machen wir uns auf den Weg, um zu erfahren, was hinter dem Link steckt.

Auf der folgenden Seite werden sogar die Daten einer Kreditkarte (Name des Karteninhabers, Kartennummer, Gültigkeit und CVV) abgefragt, um die in der E-Mail genannte ausstehende Summe von 1,95 € an UPS zu zahlen. Der Betrag ist dabei bewusst sehr niedrig gewählt, damit wir nicht lange nachdenken, sondern schnell bezahlen.

Hätten wir alle Daten gehorsam eingegeben, hätten die Initiatoren der Phishing-Mail alle Informationen, um z. B. einen Account bei einem Online-Händler einzurichten und dann auf die von uns angegebene Kreditkarte zu bestellen. Wenn Sie also noch nie gesehen haben, wie eine Kreditkarte „raucht“, geben Sie die Informationen auf einer solchen Webseite ein. Wollen Sie aber von einem größeren finanziellen Schaden verschont bleiben, lassen Sie es lieber bleiben.

Es gibt einige Anzeichen, an denen wir erkennen, ob wir einer Phishing-Webseite ausgesetzt sind:
Zunächst durch die **URL.** Auch wenn die Webseite suggeriert, dass wir die Online-Präsenz eines bekannten Unternehmens besuchen, sagt die URL etwas anderes. Entweder unterscheidet sie sich grundlegend von der für das Unternehmen erwarteten URL, oder sie unterscheidet sich nur in Nuancen, z. B. durch Hinzufügen oder Weglassen einzelner Buchstaben.

Eine nur sehr schwer zu durchschauende Methode ist dabei der Austausch von Buchstaben durch solche, die den originalen ähnlich sind. Beispielsweise kann ein „i“ durch ein „ì“ (i mit accent grave) ausgetauscht werden. Hätten Sie den Unterschied bemerkt?

Die meisten Webseiten sind mittlerweile durch ein **SSL-Zertifikat** („https“) geschützt. Hacker versuchen jedoch, diese Zertifikate zu fälschen, um ihre Opfer in vermeintlicher Sicherheit zu wähnen. Andererseits kann es auch vorkommen, dass die gefälschten Webseiten auf SSL-Zertifikate verzichten, die beim Original vorhanden sind.
Ein weiteres Indiz dafür, dass Sie auf einer gefälschten Webseite gelandet sind, ist das **falsche Logo** oder ein Logo in einer sehr schlechten Auflösung.

Vieles an der gefälschten Webseite macht insgesamt optisch nicht den Eindruck, sich auf der Original-Webseite aufzuhalten.

Auf gefälschten Webseiten werden Sie oft aufgefordert, **sensible Informationen** einzugeben. Dieser Punkt ist nicht immer eindeutig. Wer als Erstkunde einen Original-Webshop besucht, wird bei der Erstellung des Nutzeraccounts aufgefordert, die Adresse anzugeben und ein Zahlungsverfahren auszuwählen. Beides wird bei wiederholten Transaktionen nicht immer neu abgefragt. Ebenso vermeiden es Banken und Kreditinstitute, im Rahmen eines Mailings bzw. im Rahmen der Reaktion darauf, die Passwörter ihrer Kund:innen in ganzer Länge abzufragen; sie beschränken sich dabei oft auf drei oder vier Ziffern („Bitte nennen Sie die ersten drei Stellen Ihrer Online-PIN.“)

Wie bereits bei Phishing-Mails, so gilt auch bei Phishing-Webseiten, dass diese **Fehler in der Grammatik und in der Rechtschreibung** aufweisen, wenn aus dem Ausland Texte mittels Übersetzungsprogramme ins Deutsche überführt werden. Aber auch solche Programme werden immer besser.

Es ist daher wichtig, immer aufmerksam zu sein und sicherzustellen, dass Sie eine gültige Webseite besuchen, bevor Sie persönliche Informationen eingeben. Recherchieren Sie im Vorfeld in einer Suchmaschine den Namen der Firma, die Sie besuchen wollen/sollen und schauen Sie sich deren URL an, bevor Sie etwas in einer Webseite eingeben, die Sie aus einer nicht gesicherten Quelle erhalten haben.

5 TIPPS, wie Sie eine Phishing-Website erkennen

- Unbekannte URL
- Falsche Zertifizierung
- Gefälschtes Firmenlogo
- Verlangen nach sensiblen Informationen
- Schlechte Grammatik und Rechtschreibung

Sie haben auf eine Phishing-Mail reagiert – Was nun?

Haben Sie nun einmal eine Phishing-Mail erhalten und einen Link wider besseren Wissens angeklickt, dann heißt es: Ruhe bewahren und einen kühlen Kopf behalten.

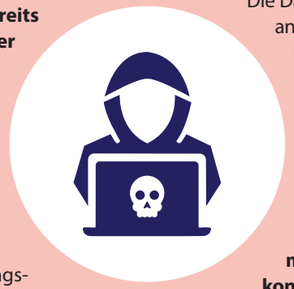
Machen Sie sich erst einmal klar, was passiert ist. Sie haben z. B. eine E-Mail erhalten. Löschen Sie diese nicht! Aus ihr kann die IT-Abteilung ableiten, was passiert ist.

Genau das sollte Ihr nächster Schritt sein:

- Geben Sie Ihrer IT-Abteilung Bescheid - warten Sie auf keinen Fall ab!
- Im Rahmen der Mail wurden Sie aufgefordert, auf einen Link/Button zu drücken. Der Mitarbeitende der IT-Abteilung wird dann unter anderem prüfen, ob etwas in Ihrem Download-Verzeichnis heruntergeladen wurde. Wenn ja, werden diese Dateien isoliert und später analysiert. In einem nächsten Schritt wird ein VirenScan Ihr komplettes System durchlaufen.
- Denken Sie anschließend darüber nach, wohin Sie durch die Betätigung des Buttons/Links geleitet wurden und welche Informationen Sie auf den folgenden Seiten eingegeben haben. Wurden Sie aufgefordert, Ihren Namen, private oder geschäftliche Zugangsdaten einzugeben oder wurden Sie nach Bankdaten oder sonstigen vertraulichen (Zahlungs-) Informationen gefragt?
- Wurden Sie aufgefordert, ein privates Passwort zu übertragen, ändern Sie das Passwort für den entsprechenden Account. Haben Sie dasselbe Passwort bei anderen Accounts eingesetzt, ändern Sie auch dort unverzüglich Ihre Passwörter. Hacker haben in der Regel den Verdacht, dass Sie sich auch bei anderen Accounts mit der von Ihnen eingegebenen Kombination aus User-ID und Passwort angemeldet haben.
- Haben Sie Kontodaten im Rahmen der Phishing-Webseite eingegeben, informieren Sie Ihre Bank oder Ihr Finanzinstitut und beobachten Sie regelmäßig ihre Kontenbewegungen auf ungewöhnliche Transaktionen.
- Nach der Aufbereitung und ggf. Abstimmung mit Ihrer IT-Abteilung löschen Sie die Phishing-E-Mail aus Ihrem Posteingang und alle Kopien, die Sie vielleicht davon gemacht haben.

Sicher vor Hackern: Handlungssicherheit mit der Phishing-Kampagne

Wir Menschen selbst sind die größte Sicherheitslücke in unseren IT-Systemen. Bereits ein Klick auf den falschen Link oder der Download einer verseuchten Datei aus einer Phishing-Mail kann Ihre komplette IT lahmlegen.



Um das zu vermeiden, haben wir eine Phishing-Kampagne entwickelt: Wir proben mit Ihren Mitarbeitenden den Ernstfall!

Das Gute daran: Von dieser Sensibilisierungsmaßnahme profitieren Ihre Mitarbeitenden auch privat. Damit wird der Nutzen für den Einzelnen schnell begreifbar – ein Wissensgewinn, der sich wiederum positiv auf Ihr Unternehmen auswirkt!

Die Phishing-Kampagne wird individuell auf die Bedürfnisse Ihres Unternehmens erstellt. Damit alle relevanten Zielgruppen in Ihrem Haus angesprochen werden, berücksichtigen wir die Auswahl eines passenden Themas und eine optimale Terminierung der Kampagne. Wir erstellen zwei professionelle Webseiten für Sie, mit denen wir den Ernstfall mit Ihren Mitarbeitenden erproben. Im Anschluss erfolgt das Tracking des Nutzerverhaltens je Teilnehmergruppe. Die Datenverarbeitung erfolgt selbstverständlich anonym. Aus den Ergebnissen erstellen unsere Experten für Cyber-Security einen umfangreichen Abschlussbericht für Sie und Ihr Management.

Wie geht es weiter? Gemeinsam mit Ihnen besprechen wir die Gefahren und Potenziale für Ihre Mitarbeitenden. Hieraus leiten wir einen Maßnahmenplan für Sie ab und geben Ihnen konkrete Hilfestellungen, wie Sie und Ihr Team Gefahren zukünftig vermeiden. Sprechen Sie uns an – wir helfen Ihnen, gegen Phishing-Attacken sicher zu sein!

Vereinbaren Sie einen unverbindlichen Beratungstermin mit unseren Phishing-Experten unter:
sales@datatree.ag

CYBERVERSICHERUNG IN DER GESETZLICHEN KRANKENVERSICHERUNG

Gastkommentar eines langjährigen DATATREE Kunden

Der GKV Spitzenverband Bund (im folgenden SpiBu) als Körperschaft des öffentlichen Rechts verhandelt bereits seit vielen Jahren Versicherungsrahmenverträge zu den Themen Vermögensschaden-Haftpflicht und Vorstandshaftung, aber auch zur Cyberversicherung.

Das erstmalige Angebot für eine Cyberversicherung wurde im Kalenderjahr 2017 über den SpiBu verbreitet. Mit dem Rundschreiben 2022/592 vom 29. September 2022 wurden dann grundlegende Anpassungen zum Gruppenvertrag Cyberversicherung mit der Allianz Global Corporate & Specialty SE kommuniziert.

Die im Schreiben genannten „erheblichen Veränderungen in den Versicherungsbedingungen" bedeuten für die meisten Krankenkassen:

- eine Verdreifachung der Versicherungsprämie
- ein massiver Anstieg des Selbstbehalts (wodurch die Schere zur Versicherungsprämie immer kleiner wird)
- eine Kürzung der Versicherungsleistungen
- eine Deckelung der maximalen Versicherungssumme in der Höhe und Anzahl
- Nachweise von Präventionsmaßnahmen zur Verhinderung von Versicherungsfällen

(beispielsweise jährliche Schulungen und Phishing Kampagnen zweimal im Jahr sowie die Vorlage eines Notfallhandbuchs)

Der sogenannte „Renewalfragebogen" ist auf mittlerweile acht Seiten angewachsen, wobei mehr als eine Seite sich mit den Hinweisen der vorvertraglichen Anzeigepflichten beschäftigt. Eine mittelgroße Krankenkasse wird vermutlich Probleme haben, den Fragebogen wahrheitsgemäß und ohne ihr Rechenzentrum beantworten zu können.

Das Lesen und Verstehen erfordert über den Alltagsgebrauch hinausgehende juristische, versicherungsrechtliche, vor allem aber IT-spezifische Kenntnisse. Versicherungsbedingungen über 29 Seiten sowie fünf weitere Seiten zur Risikobeschreibung lassen erahnen, was auf einen zukommt, wenn ein Versicherungsfall eintritt. Häufig scheinen Bedingungen bewusst schwammig formuliert, von konkreten Nachfragen ist dringendst abzuraten.

ZAHLEN, DATEN, FAKTEN

- **75% aller Unternehmen in Deutschland wurden in den letzten zwei Jahren Opfer eines Cyberangriffs**
- **58% der erfolgreichen Cyberangriffe erfolgen per E-Mail (durch Öffnen von verseuchten Anhängen oder Anklicken von Links**
- **die häufigsten Folgen sind Betriebsunterbrechungen**
- **87% der Betriebe über 50 Mitarbeitende erleiden bei einem IT-Ausfall eine mehrtägige Betriebsunterbrechungen**
- **die Hälfte der betroffenen Unternehmen benötigt bis zu drei Tage, bis die Systeme wieder vollständig laufen, 22% sogar noch länger**
- **jeder vierte Betrieb hat keine Datensicherung**

Das konkrete Risiko, das eine Krankenkasse bei einem Cyberangriff zu tragen hat, ist sehr schwierig monetär, also in tatsächlicher Euro Währung zu bemessen, da zwar die Personal- oder Sachkosten bei einem Betriebsausfall zu berechnen sind, der Reputations- und Informationsverlust sowie die Wiederherstellungskosten nicht mess oder -vorhersehbar sind.

> Fest steht aber: Das Vertrauen wird bei einer Veröffentlichung gerade bei Versicherten mit personenbezogenen Gesundheitsdaten nachhaltig verletzt.

Ein möglicherweise in der Vergangenheit in diesem Zusammenhang vernachlässigtes Risiko sind Dienstleister:innen im Krankenkassenumfeld. Dabei haben mittelgroße Krankenkassen bis zu 50 verschiedengroße Dienstleister:innen mit diversen Aufgabengebieten, die besonders schützenswerte Daten nach Artikel 9 der DSGVO verarbeiten. In den wenigsten Fällen aber wird bei Vertragsabschluss mit einem/einer Dienstleister:in nach einer Cyberversicherung gefragt. Zwar sind Krankenkassen verpflichtet, nach § 80 Abs. 1 SGB X in Verbindung mit Artikel 28 DSGVO Dienstleister:innen zu prüfen, wodurch das Risiko eines Cyberangriffs natürlich besser erkannt werden kann, eine Konsequenz bis zur Aufforderung eines Abschlusses einer Cyberversicherung ist derzeit jedoch nicht vorgesehen.

Wurde die Anpassung des Vertrages im Oktober 2022 noch mit einem Anstieg der Versicherungsfälle außerhalb der GKV begründet, wurden seitdem drei gravierende Hackerangriffe im GKV nahen Umfeld bekannt: Wilken im Oktober 2022 unmittelbar nach Veröffentlichung des Rundschreibens, Bitmarck und Adesso im Februar 2023.

Die Furcht vor einem Kumulschaden - ein Ereignis, das bei allen Versicherten den Versicherungsfall auslöst - ist seitdem nicht mehr von der Hand zu weisen. Auch das Verhalten der Gematik beispielsweise zu den Themen eGK und elektronisches Rezept trägt zu einem Ausbau des Vertrauensverhältnisses nicht bei.

Stellungnahme von Prof. Dr. Thomas Jäschke

Professor für Medizininformatik und Vorstand der DATATREE AG

Gelangen sensible Kund:innendaten von Krankenkassen in unbefugte Hände und werden durch einen Cyberangriff ins Darknet gestellt – so wie es im vergangenen Jahr bei fast zehn Millionen Kundendaten der australischen Versicherung Medibank der Fall war – ist hier sicher von einem „worst case“ zu sprechen. Es ist sowohl mit einem erheblichen Imageschaden und Vertrauensverlust zu rechnen, als auch mit einem hohen finanziellen Schaden, um IT-Systeme wieder herzustellen und abzusichern.

Eine Cyberversicherung, die finanziellen Schaden zumindest teilweise übernimmt, erscheint hier zunächst sinnvoll. Ist die Versicherung jedoch an komplexe Auflagen und für das Personal mit nahezu unüberwindbaren Hindernissen sowie negativen Auswirkungen auf die Versicherungspolice für Kund:innen verbunden, steht schnell die Sinnfrage im Raum: Ist die Versicherung unter solch erschwerten Bedingungen, wie sie im Rundschreiben des SpiBu deutlich wurden, tatsächlich nötig? Wichtig ist eine vernünftige Grundlage.

Eine Cyberversicherung kann im Rahmen des Business Continuity Managements eine unterstützende Maßnahme innerhalb des Risikomanagements sein. Ob sie wirklich sinnvoll ist und mehr Vor- als Nachteile bringt, sollten Experten entscheiden, die beispielsweise durch ihr Know-how den Renewalfragebogen korrekt beantworten und beurteilen, ob eine Krankenversicherung entsprechende Auflagen erfüllen kann.

Diese Ressourcen können gesetzliche Krankenkassen in den meisten Fällen nicht selbst leisten. Externe Dienstleister:innen müssen hier unterstützend einwirken und die Gesamtsituation aus Expertensicht zu beurteilen.

Die DATATREE AG berät Unternehmen hinsichtlich ihres Bedarfs und ihrer Möglichkeiten und baut ein Informationssicherheitsmanagementsystem auf. In diesem Rahmen dieser ganzheitlichen Perspektive ist auch die Beurteilung einer möglichen Cyberversicherung möglich.

AKTUELLES VON DER DATATREE AG

DATATREE AG verstärkt Vorstandsteam

Seit dem 01.04.2023 ist Thomas Bödeker Mitglied des Vorstandes der DATATREE AG und verstärkt die Unternehmensleitung, zusammen mit Prof. Dr. Thomas Jäschke. Der neue Chief Operation Officer (COO) wird zukünftig für das strategische und operative Management zuständig sein.

Der Wirtschaftsjurist bringt über 30 Jahre Erfahrung aus den Bereichen medizinische Dienstleistungs- Health Care und Life Science mit und gilt als Führungspersönlichkeit der deutschen Wirtschaft.

Thomas Bödeker
Mitglied des Vorstandes der DATATREE AG

In den letzten zehn Jahren hielt er geschäftsführende Positionen beim Grönemeyer Institut für MikroTherapie, dem DRK-Blutspendedienst West gGmbH sowie zuletzt bei der unimed Abrechnungsservice für Kliniken & Chefärzte GmbH. „Ich freue mich in einem so wegweisenden und zukunftsträchtigen Themenfeld wie der Informationssicherheit die notwendige Digitalisierung im Gesundheitswesen zielgerichtet mitzugestalten”, sagt Bödeker, „mich erwartet ein großartiges Team, mit dem wir gemeinsam viel bewegen wollen.“

DATATREE AG erhält Zuschlag der Prospitalia GmbH für Implementierung von Informationssicherheitssystemen in Krankenhäusern

Die DATATREE AG erhielt im Rahmen einer europaweiten Ausschreibung den Zuschlag der Prospitalia GmbH. Der Dortmunder Compliance Provider bietet damit zukünftig seine Unterstützung beim Aufbau und Vertrieb von Informationssicherheitsmanagementsystemen (ISMS) in den von Prospitalia betreuten Krankenhäusern an.

„Wir freuen uns sehr darüber, in der DATATREE AG eine geeignete Partnerin gefunden zu haben, die seit über zehn Jahren die Informationssicherheit und den Datenschutz im Gesundheitswesen vorantreibt“, so Henning Hahn, zuständig für Invest Consulting der Prospitalia GmbH.

Wir sehen uns auf der DMEA

Digitalisierung und Informationssicherheit – ganzheitlich, effizient, sicher

Das Gesundheitswesen der Gegenwart und der Zukunft ist das digitale Gesundheitswesen, basierend auf groß angelegten und komplexen Datenmengen mit vielzähligen Behandlungs- und Forschungsmöglichkeiten.

Grundlage für die optimale Nutzung dieser Datenmengen sind die Informationssicherheit und der Datenschutz und die damit einhergehenden Sicherheitsmechanismen sowie weiterführende gesetzliche und normative Regelungen. Es handelt sich nach wie vor um einen Bereich mit vielzähligen Konfliktthemen, der mehr Handlungssicherheit in der Praxis benötigt. Es bedarf Experten, die Leitplanken für die Zukunftsmedizin setzen.

WIR MACHEN DAS FÜR SIE - Informationssicherheit, IT-Sicherheit und Datenschutz

Die DATATREE AG bietet mit ihren Experten eine aus über 30 Jahren resultierende Expertise im Gesundheitswesen und arbeitet erfolgreich mit ihren Kund:innen an einem sicheren Gesundheitswesen der Gegenwart und der Zukunft. Sie möchten mehr über unsere Dienstleistungen und konkreten Produkte erfahren?

Wir sehen uns auf der DMEA in Halle 3.2 | A-104

DMEA Berlin 25.–27. April 2023 Connecting Digital Health

24. Fachtagung setzt Leitplanken für den Datenschutz in der Zukunftsmedizin

Unter dem Kernthema „Datenschutz in der Medizin“ kamen am 23. Februar 2023 über 40 Vertreter:innen aus dem Gesundheitswesen im Rahmen der 24. Fachtagung „Update BDSG – Datenschutz in der Medizin“ zusammen.

Im Dortmunder NH Hotel trugen namhafte Referierende den aktuellen Stand aus Forschung und Praxis vor und boten Raum für Fragen und Diskussion mit den >>>

AKTUELLES VON DER DATATREE AG

Teilnehmenden. Die Veranstaltung war ein voller Erfolg und ein wichtiger Schritt, um in den Dialog zu treten.

Referent:innen v.l.n.r.: Dipl. Psych. Dr. rer. nat. Johannes Drepper Referent der TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V., Prof. Dr. Thomas Jäschke, Professor für Medizininformatik und Vorstand DATATREE AG, Betram Raum, ehem. Leiter Fachreferat Gesundheit beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Bonn, Dr. med. Anke Diehl Chief, Transformation Officer und Leiterin Stabsstelle Digitale Transformation an der Universitätsmedizin Essen, Manfred Weitz, Schirmherr, Agentur esturias, Dr. Patrick Guidato, Clustermanager Cluster Medizin.NRW), Anja Burmann, M.Sc. Stv. Abteilungsleiterin HealthCare am Fraunhofer-Institut für Software- und Systemtechnik ISST

Erfolgreicher Jahresauftakt: DATATREE AG begrüßt Prüfgemeinschaft der Krankenkassen

Unter dem Motto „Digitalisierung und Informationssicherheit – ganzheitlich, effizient, sicher" hatte die DATATRE AG 34 zugehörige Krankenkassen der Prüfgemeinschaft zum Neujahrsempfang nach Dortmund eingeladen.

„Insgesamt durften wir feststellen, dass der Austausch für die Verantwortlichen einen großen Mehrwert bietet, um gezielt die wichtige Aufgabe der Informationssicherheits- und Datenschutzbeauftragten der Krankenkassen voranzubringen und gemeinsam Synergien zu schaffen", zieht Nina Kill, Bereichsvorstand Marketing & Kommunikation und Koordinatorin der Veranstaltung, das Fazit der Veranstaltung, „wir, als erfahrener Compliance Provider werden genau das vorantreiben. Wir verstehen unsere Aufgabe nicht nur darin, durch konkrete Audits zu unterstützen, sondern auch die Rollen des ISB und DSB in ihrer Relevanz zu untermauern."

Neue starke Partnerschaft: DATATREE AG und nexac dental communications setzen Paket zur sicheren Arztpraxis erfolgreich um

Das Komplettpaket für eine "Sichere Arztpraxis" wurde bereits in einigen Praxen erfolgreich umgesetzt.

Nun bietet die DATATREE AG das Angebot gemeinsam mit einem weiteren Vertriebs- und Servicepartner, Uwe Gösling von nexac dental communications an, um weiteren Praxen die Umsetzung von Informationssicherheit, IT-Sicherheit und Datenschutz zu ermöglichen.

nexac dental communications
www.nexac-campus.com

Neue Anforderungen für Cyber Security - EU NIS 2 Cyber Security

EU NIS2 ist der europäische Rahmen für Betreiber:innen Kritischer Infrastrukturen und legt Cyber Security Mindeststandards in der EU fest. NIS2 (EU 2022/2555) erweitert die Betroffenheit und Pflichten deutlich – ab 2024 müssen viele Unternehmen in 18 Sektoren ab 50 Mitarbeitenden und 10 Mio. EUR Umsatz in Cyber Security umsetzen.

Die DATATREE AG bereitet bereits jetzt ihre Kund:innen auf die bevorstehenden Anforderungen vor. Bereits im März 2023 besuchten viele Klinikvertreter hierzu den kostenlosen Roundtable zum Thema Datenschutz, Informationssicherheit und IT-Sicherheit im Gesundheitswesen. Der nächste Roundtable findet am 5. Mai 2023 statt. Folgen Sie uns hierzu bei LinkedIn.

Sie möchten keine Neuigkeiten mehr verpassen und regelmäßig Updates zu den Themen Informationssicherheit und Datenschutz erhalten?

Abonnieren Sie hier unseren Newsletter. Jetzt anmelden und auf dem Laufenden bleiben.

Sie möchten die ExperSite regelmäßig kostenlos erhalten?

Dann schicken Sie eine Mail mit Ihren Kontaktdaten und dem Betreff „Exper*Site*" an Ihre Ansprechpartnerin Nina Kill, nina.kill@dr-jaeschke.ag.

Sie möchten auf dem Laufenden bleiben, wenn es um die Themen Informationssicherheit und Datenschutz geht?
Dann abonnieren Sie hier den Newsletter der DATATREE AG über den QR-Code oder unter: www.datatree.ag/blog

Vielen Dank für Ihr Interesse.

Impressum

ExperSite Ausgabe 01 2023 | **ISSN-Print** 2364-5636 | **ISSN-Internet** 2364-5644 | **Herausgeber:** DR. JÄSCHKE AG, Märkische Straße 212-218, 44141 Dortmund, T +49 231 964193-0 office@dr-jaeschke.ag | www.dr-jaeschke.ag | Sitz der Gesellschaft: Dortmund | **Registergericht:** Amtsgericht Dortmund | **Registernummer:** HRB 27509 | **Umsatzsteuer-Identifikationsnummer:** DE300625711 | **Vorstand:** Prof. Dr. Thomas Jäschke, Angelica Morina, B.A. | **Vorsitzende des Aufsichtsrates:** Dr. Anke Diehl | **Inhaltlich Verantwortlicher gemäß § 1 Abs. 4 TMG, § 55 Abs. 1 RStV und § 55 Abs. 2 RStV:** Prof. Dr. Thomas Jäschke | **Redaktionsleitung:** Nina Kill | **Design und Umsetzung:** Silvia Lorenz | **Druck:** www.onlineprinters.de | **Auflage:** 5.000 | **Fotos: AdobeStock:** Seite 1/4 © studiostoks, Seite 8 © hasan, Seite 12 © ipopba, Seite 18 © TarikVision, Seite 19 © madedee, Seite 21 © Juli, Seite 23 © HNFOTO | **istockphoto:** Seite 5/7: © Intpro, Seite 27 © Sam Edwards | **JÄSCHKE GRUPPE:** Seiten 25/26 © Marina Lutsyuk

www.linkedin.com/company/jaeschke-gruppe

www.instagram.com/jaeschke_gruppe/

Magazin_HP1_ExperSite-01-23_v1.0

Exper*Site* ist das Magazin der JÄSCHKE GRUPPE für
Digitalisierung, Informationssicherheit und Datenschutz

www.dr-jaeschke.ag