www.comply-online.de
6. JAHRGANG
DEZEMBER 2021
SEITEN 1–64
ISSN 2364-7604

comply.

FACHMAGAZIN FÜR COMPLIANCE-VERANTWORTLICHE

IM BRENNPUNKT

Compliance-Risiken 2022

> Update: Arbeitsrechtliche Compliance

> Kartellrechts-Compliance – aktuelle Entwicklungen

> Datenschutz-Compliance

> Update: Tax Compliance

> Das FISG als Ziehvater der „dotted line" für Compliance an den Aufsichtsrat

REGULARS

> **Geldwäscheprävention**

> **IT-Compliance**

> **Whistleblowing**

> **Sustainability**

ESSENTIALS

SERVICES

Compliance-Risiken 2022

4/2021

IN KOOPERATION MIT:

Viadrina Compliance Center

DICO Deutsches Institut für Compliance

COMPLIANCE ACADEMY

Reguvis

Interview

Ein Plädoyer für sichere IT-Systeme, staatliche Schutzversprechen sowie gegen manipulierbare Saugroboter

Im Gespräch* mit Ramon Mörl, Geschäftsführer der itWatch GmbH, deren Fokus auf dem Schutz vor Datendiebstahl (Data Loss Prevention – DLP), auf technischen Vertrauensketten sowie deren organisatorischer Einbettung durch rechtsverbindliche Dialoge, Endgeräte-Sicherheit (Endpoint Security), Datenschleusen mit Datenwäsche sowie Mobile Security und Verschlüsselung liegt.

comply.: *Herr Mörl, wie sicher sind Ihre Zielgruppen mit dem Thema IT-Security? Treffen Sie eher auf IT-Security-Experten oder auf Neueinsteiger, also auf grundsätzlich Ratsuchende?*

Ramon Mörl: Wir können mehrere Zielgruppen unterscheiden. Zum einen gibt es die „alten Hasen", die wir hauptsächlich bei Familienunternehmen mit wenig Fluktuation und bei Kunden antreffen, in deren Umfeld IT-Sicherheit schon immer wichtig war – z. B. Polizei, Militär und Nachrichtendienste. Dann gibt es klassische Mainstream-Kunden, die den Weg nur selten zu „best oft the breed"-Lösungen schaffen. Bei diesen wechseln die IT-Mannschaft und die IT-Security-Verantwortung regelmäßig, sodass es kein nachhaltig bewirtschaftetes Thema ist. Die dritte Gruppe sind die Newcomer. Meist sind das Unternehmen, bei denen die IT-Sicherheit durch einen Vorfall direkt im Haus oder in deren Nähe spontan an Wichtigkeit gewinnt. Die Personen in diesen Unternehmen sind meist Neueinsteiger in das Thema oder waren bisher mit anderen Themen betraut, denn „das mit der IT-Sicherheit kann ja auch nicht so schwer sein".

Bei den beiden letzten Zielgruppen zeigt sich die Wichtigkeit Ihrer Frage. Im gesamten Entscheidungsprozess fehlt die Entscheidungskompetenz darüber, was „wirklich immer schützt" und „was nur manchmal oder meistens schützt". Die Frage nach der Mechanismusstärke des Schutzes und der darüber erzielbaren Resilienz gegenüber Angriffen ist aber nach meiner Erfahrung das Entscheidende bei der Beschaffung und Implementierung von Schutzprodukten. Lassen Sie mich ein Beispiel dafür nennen, dass es nicht immer nur an der Kompetenz der technischen Abteilung liegt: Wir hatten bei einem DAX-Unternehmen eine sechsmonatige Testphase von mehreren Produkten – das itWatch-Produkt war eines davon. Die Testmannschaft war sehr gut informiert und hat sehr komplizierte Tests durchgeführt und kam nach sechs Monaten zu dem Schluss, das itWatch-Produkt als „best oft the breed" zu kaufen. Der Einkauf veränderte das Szenario und organisierte eine Internetversteigerung – unabhängig von der Mechanismusstärke des Produktes, also nur nach dem Preis. Das billigste Produkt gewann. In der Konsequenz hat man die Anforderungen an den Einsatz nachträglich nach unten gesetzt, weil das bestellte Produkt nicht geeignet war für den Roll-out.

comply.: *Würden Sie sagen, dass das auf dem Markt derzeit angebotene IT-Sicherheits-Produktangebot den Herausforderungen, die sich durch immer neue Sicherheitslücken und Angriffstechnologien ergeben, gerecht wird?*

Ramon Mörl: Ein klares Nein. Es gibt eine ganze Menge von Produkten, die den Anforderungen durch immer neue Angriffe wirklich gerecht werden – aber der Nutzer kann diese nicht von „Fake Security"-Produkten unterscheiden. Produkte, deren Hersteller ihr Kapital zu großen Teilen für Marketing und zu geringem Anteil für die technisch notwendige Forschung ausgeben, bleiben häufig in dem Schutzversprechen hinter der Erwartung des Marktes zurück. Aber einmal gekauft wird das Thema frühestens nach drei Jahren wieder „angefasst". Leider ist dadurch auch der Markt für sinnvolle Lösungen oft für längere Zeit blockiert.

Ein Beispiel dafür kann beim Thema „Sandboxing und Virtualisierung" beobachtet werden. Hier haben sich viele sinnvolle und auch weniger sinnvolle Lösungen einen Markt erarbeitet. Die wenigsten Kunden realisieren aber, wenn sie z. B. auf Applikationsvirtualisierung setzen, dass der Content, der in den Applikationen bearbeitet wird, dann doch z. B. für die Druckaufbereitung in die produktiven Netze kommt, weil bei den gängigen Lösungen nicht alle Hintergrundprozesse virtualisiert werden. Aus diesen Gründen hatte das BSI, als es das ReCoBS-Profil für den sicheren Einsatz von Browsern[1] veröffentlichte, auch bestimmte Verfahren ausgenommen.

** Das Gespräch führte Richard Huber, Sicherheitsforscher mit dem Schwerpunkt IT-Compliance am Fraunhofer Institut für Offene Kommunikationssysteme (FOKUS) in Berlin.*

comply.: *Herr Mörl – was fehlt Ihrer Meinung nach am dringlichsten im Markt für IT-Sicherheitsprodukte und -dienstleistungen und wo erkennen Sie in diesen Defiziten die gravierendsten Einfallstore in IT-Infrastrukturen bzw. Fallen für den Faktor Mensch?*

Ramon Mörl: Herr Schönbohm, der Präsident des BSI, und viele andere für die IT-Sicherheit wichtige Personen und Organisationen betonen immer wieder, dass wir nur dann gegen die Angriffe geeignet gerüstet sind, wenn wir zusammenarbeiten. Dieser Erkenntnis stimme ich zu 100 % zu – leider wird sie nicht gelebt und was noch schlimmer ist, die tatsächlichen Maßnahmen sind oft kontraproduktiv. In dem IT-Sicherheitsgesetz 2.0 und den weiteren Regulierungen dazu wird z. B. sehr stark auf Diversität gesetzt, um nach erstem Verständnis unabhängig zu sein und immer einen Dienstleister zu haben, der in die Leistung geht. Dabei wird aber verkannt, dass die Ziele Verfügbarkeit auf der einen Seite und Integrität und Vertraulichkeit auf der anderen Seite häufig im Gegensatz zueinander stehen. Ein einfaches Beispiel: Man möchte alle Dateien auf allen Servern verschlüsseln, um auch in anderen Regionen speichern zu können. Um nicht abhängig von einem Produkt und einem Dienstleister zu sein, kauft man zwei Produkte von zwei Lieferanten und fordert Kompatibilität, sodass mit jedem der beiden Produkte alle Dateien entschlüsselt werden können. Hat nun auch nur eines der beiden Produkte eine Hintertür oder eine Schwachstelle, so sind alle Daten – auch die von dem zweiten verschlüsselten – offengelegt. Der Verlust der Vertraulichkeit wurde also dem Ziel der Verfügbarkeit „geopfert", obwohl das Produkt eigentlich Vertraulichkeit sichern sollte.

Was heißt das jetzt für den Faktor Mensch? Bruce Schneier, ein Urgestein der Kryptografie, sagte in einer emotionalen Rede auf der Münchner Cyber Security Konferenz (mcsc), die immer einen Tag vor der Münchner Sicherheitskonferenz (msc) stattfindet, dass wir aufhören müssen, den Anwender vor bestimmten Aktionen in der IT zu warnen (USB-Sticks, E-Mail-Anhänge und Browser-Downloads) und endlich anfangen müssen, sichere IT-Systeme zur Verfügung zu stellen, sodass sich der Anwender ohne schlechtes Gewissen auf seine Tätigkeit konzentrieren kann. Das ist eine kooperative Anstrengung. Wenn wir uns den Straßenverkehr ansehen, dann stellen wir fest, dass auch dort etwas passieren kann, aber über die letzten 100 Jahre wurden viele Regeln eingeführt, die die Unfallhäufigkeit, aber auch den entstehenden Schaden reduzieren. Dazu tragen viele Themen bei. In der IT haben wir kaum die Möglichkeit für Haftung und es gilt ein „Schütz Dich selbst, sonst schützt Dich niemand". Die Steuergelder werden nicht zum Schutz der Bürger und ansässigen Unternehmen im Cyberraum ausgegeben. Auch an dieser Stelle halte ich Kooperation für zwingend notwendig.

comply.: *Was sind denn die derzeit größten Bedrohungen im IT-Sicherheitsbereich?*

Ramon Mörl: Auf der it-sa habe ich gerade einen Vortrag mit dem Titel „Jeder Cyberangriff braucht Soft- oder Hardware – z. B. Ransomware einfach rauswaschen – wie geht das?" gehalten. Ich denke, die größte Bedrohung ist, dass viele neue Technologien, die neue Fähigkeiten, mehr Spaß, einfacheren Betrieb, weniger Ärger oder Ähnliches versprechen, eben auch neue Tore öffnen. Zum Beispiel Codeelemente, also kleinste Stückchen Software, die in IT-Werkzeuge integriert werden und bei denen sich niemand Gedanken macht, wie wir darin Gut von Böse unterscheiden können. Am Ende des Tages muss man aber, wenn man seine IT-Umgebung sicher managen will, jedes Stückchen Software und die in der Hardware verbauten Elemente wie ein Controller kennen, denn man kann nur managen, was man kennt.

comply.: *Wie hoch schätzen Sie das Sensibilisierungslevel gerade bei IT-ferneren Organisationen und Wirtschaftsunternehmen hinsichtlich Gefahren, Schäden und einer klaren Risikoabschätzung ein?*

Ramon Mörl: In Ihrer ersten Frage hatte ich bereits drei Kategorien aufgemacht. Familienunternehmen mit guten Margen sind sich ihrer Stellung bewusst und versuchen ihren Besitz sowie auch die IP und ihre intellektuellen Assets geeignet zu schützen.

Bei Managern, die ihre Position meist nach drei Jahren wechseln, ist das Erfüllen der eigenen Ziele für ihre Boni höherwertig, sodass hier oft nicht nachhaltig gearbeitet wird. Insofern hat es nach meiner Wahrnehmung weniger mit der Branche oder der Distanz zur IT zu tun.

Etwas ist aber auffällig: Durch die Digitalisierung von Standardprodukten, wie Staubsaugern, Lampen, Rauchmeldern etc., kommt das IT-Risikomanagement des Herstellers dieser Produkte bis ins Schlafzimmer der Kunden. Stellen Sie sich vor, Sie wissen, welches Modell eines Staubsaugerroboters ihr Nachbar einsetzt. Sie gehen in den Laden, kaufen ein baugleiches, öffnen es und setzen eine Kamera, ein Mikro und ein WLAN ein. Sie schicken es an ihren Nachbarn, zusammen mit einem Entschuldigungsschreiben des Herstellers, dass in dem alten Modell leider der Akku überhitzen kann, und schon haben Sie fahrbare Augen und Ohren in allen Zimmern ihres Nachbarn.

Nach meiner Wahrnehmung müsste sich der Hersteller um seine Kunden sorgen, das Risikomanagement für sie übernehmen und sie gegen Angriffe schützen. Dann wäre sein Produkt aber teurer und später auf dem Markt. Wie können wir also bei der Digitalisierung der Gesellschaft rote Linien ziehen und das Filmen in fremden Schlafzimmern nicht dem Risikomanagement eines Staubsaugerherstellers überlassen?

comply.: *Starkes Beispiel, Herr Mörl! Wir sind gespannt, wie viele unserer Leserinnen und Leser nach diesem Statement ihre Saugroboter mal ganz genau unter die Lupe nehmen werden. Sagen Sie – wie sieht es mit diesem Bewusstsein bei Behörden, Kommunen und überhaupt bei öffentlichen Auftragnehmern aus?*

Ramon Mörl: Wahrscheinlich treffen wir hier die größte Diskrepanz zwischen Wunsch und Wirklichkeit an. KMU in jeder Region nehmen sich ihre Kommunen und kommunalen Unternehmen oft als Vorbild, denn die wissen genau, was Gesetz ist und bekommen ganz sicher gesagt, wie man die IT schützt. Leider ist das aber nicht so.

Ergebnisse von Marktuntersuchungen einer Behörde, die mit Steuergeldern finanziert wurden, stehen anderen steuerkonsumierenden Organisationen nicht zur Verfügung. Insofern bekommt die Kommune leider keinen Hinweis vom BND, dem BKA oder ihrer lokalen Polizei, welche IT-Sicherheitsprodukte einen guten Schutz bieten, sondern sie muss sich auf die Expertise der eigenen Mitarbeiter oder die Gespräche in verschiedenen Gremien verlassen. Alle Gremien sind aber zur Neutralität verpflichtet, so wird der Städte- und Gemeindetag dieses Defizit auch nicht beheben.

Die IT-Sicherheit ist in diesem Punkt deshalb anders, weil es keine definierte Metrik und keine sichtbare Funktionalität gibt. Bei anderen IT-Produkten erkennt man relativ leicht, ob sie ihre Funktion, für die man sie einkaufen will, auch leisten. Bei IT-Sicherheit eben nicht. Deshalb wäre es besonders wichtig, die Mechanismusstärke von Produkten in den Gremien darzustellen.

comply.: *Könnte die Forschung da helfen? Was wünschen Sie sich von der IT-Sicherheitsforschung?*

Ramon Mörl: Drei Dinge wären mir besonders wichtig: Erstens sollte dringend an Verfahren zum Messen der Robustheit gearbeitet werden – also wie gut schützt ein Produkt. Zweitens müssen die Forschungsergebnisse sinnhaft in die Nutzung überführt werden. Es hilft uns nicht, wenn wir Forschungsweltmeister sind, aber keine Wertschöpfung aus den Forschungsergebnissen stattfindet. Drittens: Wenn wir feststellen, dass etwas, was wir uns gewünscht haben, nicht so funktioniert, wie wir dachten, dann müssen wir interdisziplinär anfangen zu forschen, was noch fehlt.

Dazu ein paar Beispiele: Wenn wir feststellen, dass wir durch Weitergabe der Marktsichtungsergebnisse zwischen steuerkonsumierenden Organisationen zum einen Geld sparen können und zum anderen höhere Sicherheit erreichen, dann darf der Einwurf „das Vergaberecht steht dem Austausch entgegen" nicht verhindern, sondern muss zum Forschen anregen, wie wir es hinbekommen. Wenn Frau Merkel ihr sicheres Handy nicht nutzt, weil die Sicherheitsfunktionen ihre Ergonomie beeinträchtigen, müssen wir forschen, wie wir das Handy „Kanzlerin-tauglich" machen.

comply.: *Da sind wir fast schon bei meiner nächsten Frage – die Politik – was würden Sie sich von dieser wünschen?*

Ramon Mörl: In erster Linie mehr Kooperation. Dazu zählt, dass der Staat ein Schutzversprechen gegenüber seinen Bürgern und den ansässigen Organisationen abgibt, dieses aber im Cyberraum nicht erfüllt. Wieder stehen natürlich viele Gründe gegen einen Schutz aller Bürger im Cyberraum, aber wenn wir nicht anfangen, dazu zu forschen und nachzudenken, wie wir einen Basisschutz und eine starke Reduzierung der Cyberkriminalität als Gesellschaft hinbekommen, dann wird die Digitalisierung auf zweifelhaftem Boden gebaut.

comply.: *Herr Mörl – abschließend noch meine üblichen drei Abschlussfragen zu Ihrem persönlichen Verhalten in der IT Security: Wie sicher fühlen Sie sich selbst im Umgang mit Ihren individuellen Aufgaben, Prozessen und Technologien – gerade auch vor dem Hintergrund des Arbeitens im Homeoffice?*

Ramon Mörl: Bestens gerüstet. Ich beschäftige mich seit 30 Jahren mit IT-Sicherheit als Kernthema, da ist es tatsächlich egal, wo ich arbeite. Das adäquate Schutzniveau kann ich immer gut einhalten – allerdings verzichte ich auf viele „Innovationen", die mir verdächtig erscheinen.

comply.: *Und wie ausgeprägt ist Ihre Bereitschaft zu Einbußen in der Bequemlichkeit zugunsten eines höheren IT-Sicherheitslevels?*

Ramon Mörl: Natürlich bin ich bereit zu einem anderen Verständnis. Ich benutze drei Handys und mehrere Rechner. Ich würde nie eine Videokonferenz nativ auf meinem Firmenrechner durchführen oder meine Authentifizierung zu Firmenkonten (auch E-Mail) auf einem fremden Rechner vornehmen.

comply.: *Zum Schluss eine schwierige Fachfrage: Was verstehen Sie unter einer Advanced Persistent Threat?*

Ramon Mörl: Es handelt sich um eine hochwertige, dauerhaft präsente Bedrohung, die unterschiedliche Angriffsvektoren nutzt, um immer weiter in ein System oder eine Organisation einzudringen. Hochwertig deshalb, weil nicht die sofortige Monetarisierung gesucht wird – wie beispielsweise bei Ransomware – und deshalb sehr viel Wert auf Verschleierung des Angriffs gelegt wird. Dauerhaft präsent deshalb, weil tatsächlich echte Menschen mit Know-how auf der anderen Seite sitzen und sich die Abfolge der Angriffe so ausdenken, wie es gerade passend erscheint, sodass der Angriff insgesamt erfolgreich wird. Es entsteht also eine Folge von aufeinander aufbauenden Angriffen, die insgesamt ein längerfristiges Ziel verfolgen und während dieses Zeitraums nicht erkannt werden dürfen.

comply.: *Herr Mörl – haben Sie vielen Dank für Ihre Zeit und für das Gespräch.*

1 Vgl. dazu https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/recobslanginfo_pdf.pdf?__blob=publicationFile.