Jahresrückblick 2020:
Das Jahr aus Sicht der Cybersicherheit

„There are only two types of companies:
those, that have been hacked,
and those, who don’t know,
they have been hacked.“

—

John T. Chambers

Jahresrückblick Cybersicherheit

carmasec

Wer auf das Jahr 2020 zurückblickt, der wird nur an ein Thema denken: Corona. Diese Pandemie hat das Leben aller rund um den Globus bestimmt wie kein anderes Ereignis zuvor. Sie hat uns unvorbereitet getroffen. Allen voran hat sie uns vorgeführt, welche Defizite Unternehmen in Sachen Digitalisierung und in Sachen Cybersicherheit aufweisen. Die Pandemie war die Gelegenheit für Cyberkriminelle für Spionage, Sabotage und Betrügereien.

Sie hat auch gezeigt, dass Notfallpläne fehlen, Unternehmen für ortsunabhängiges Arbeiten der Beschäftigten nicht gut ausgestattet sind und die Mitarbeiter selbst Schulungsbedarf haben, um nicht auf die Methoden der Kriminellen hereinzufallen.

Jahresrückblick Cybersicherheit

carmasec

Doch wo Schatten ist, muss auch eine Sonne sein. Der in 2019 gegründete Weisenrat für Cybersicherheit hat dieses Jahr der Bundesregierung seinen ersten Bericht vorgelegt. Ein wichtiger Schritt auf dem Weg, die Fähigkeiten auf diesem Gebiet auszubauen. Ganz wichtig: Cyber-Resilienz hat an Bedeutung gewonnen. Sie hilft, sich sowohl über die Bedrohungslagen in der Digitalisierung bewusst zu werden als auch Unternehmen Instrumente, Konzepte und Strategien an die Hand zu geben.

2020 mag ein schwieriges Jahr gewesen sein. Die Lichtblicke, die dieses Jahr durchscheinen, werden in 2021 helfen, einige Herausforderungen besser zu bewältigen.

Januar 2020

Allianz Risk Barometer 2020: Cyberangriffe größte Gefahr für Unternehmen

Zum Allianz Risk Barometer 2020

Erstmals in der neunjährigen Geschichte des Allianz Risikobarometers führt in diesem Jahr die Angst vor Cyberattacken weltweit die Rangliste an. Auf Grundlage der Einschätzung von 2.700 internationalen Risikoexperten aus über 100 Ländern veröffentlicht die Allianz Global Corporate & Specialty einen Bericht zu den bedeutendsten Gefahren für Unternehmen. Die Experten spiegeln, was auch die Medienberichterstattung der letzten Monate zeigte: Cyberrisiken sind die größte Bedrohung des Jahres. Somit verdrängten Cyber-Vorfälle den letztjährigen Tabellenführer, das Risiko einer Betriebsunterbrechung, vom ersten Platz. Die Sorge vor Betriebsunterbrechungen war seit 2013 der Anführer des Rankings - damals lagen Cyberattacken mit 6 Prozent gerade einmal auf dem 15. Platz.

In Deutschland hingegen liegt noch immer die Angst vor Betriebsunterbrechungen mit 55 Prozent auf Platz eins - jedoch direkt gefolgt von Cyber-Vorfällen (44 Prozent).

Februar 2020

Für Online-Unternehmen steigt die Relevanz der Cybersicherheit stetig an

Zum Artikel von Infopoint Security

Das Thema Cybersicherheit könnte in der heutigen Zeit kaum wichtiger sein: Mehr Menschen denn je sind durch Geräte miteinander vernetzt und auch das Internet gewinnt weiterhin an Relevanz. Obwohl diese Vernetztheit viele Vorteile bietet, geht mit ihr ebenso eine Zunahme an möglichen Sicherheitslücken und eventuellen Betrugsangriffen einher.

Für Unternehmen ganz gleich welcher Größe wird die Frage nach Cyber-Security somit wichtiger denn je. Nur vertrauenserweckende Online-Unternehmen, die für Daten und Verbraucher eine sichere Umgebung darstellen, gewinnen das Vertrauen von Kunden – und können so erfolgreich sein. So fand das Finanzunternehmen WorldPay in einer Studie heraus, dass rund 24 Prozent aller Online-Einkäufer Transaktionen im Internet nicht abschließen, wenn ihnen ihre Sicherheit während des gesamten Einkaufs nicht gewährleistet wird. Besonders Kunden, die sich mit Prozessen im Netz auskennen, achten auf die Korrektheit von Online-Businesses.

März 2020 (1)

Die Corona-Pandemie als Nährboden für Cyber-Kriminalität

Zum Artikel von Zeit Online

Die Corona-Pandemie zwingt seit Anfang des Jahres Arbeitnehmer ins Homeoffice. Für sie ist es die sicherste Option - für ihre Computer jedoch nicht unbedingt. Denn Cyberkriminelle jeglicher Art machen sich die Situation zunutze. Sie profitieren von der Unsicherheit und Angst ihrer Mitmenschen. So wurde Anfang März beispielsweise vom Securityspezialisten Shai Alfasi ein Programm entdeckt, welches verspricht, die aktuellen Fallzahlen von Covid-19 anschaulich darzustellen. Zusätzlich fungiert das Programm jedoch als Trojaner "Azorult", der eine Schadsoftware ist. Die macht sich nach der Aktivierung durch den Nutzer auf die Suche nach rentablen Informationen - Kreditkarteninformationen etwa, aber auch Passwörter fallen darunter. Diese Masche ist kein Einzelfall. So wurde eine Android-App entdeckt, die ebenfalls vorgab, die aktuellsten Informationen zum Coronavirus zu präsentieren. Stattdessen aber sperrte die App das Smartphone und forderte von Besitzern eine Zahlung in Höhe von 100 Dollar, um das Smartphone wieder freizugeben.

März 2020 (2)

Deutschland-Umfrage: IT- Sicherheitsmaßnahmen im Home-Office ausbaufähig

In einer deutschlandweiten Online-Umfrage hat der Bundesverband IT-Sicherheit e.V. (TeleTrusT) im März ermitteln lassen, welche Sicherheitsvorkehrungen Nutzer des Home-Office getroffen haben. Das Ergebnis weist darauf hin, dass die Befragten durchaus ein Bewusstsein für mögliche Risiken haben – die technische Umsetzung aber noch ausbaufähig ist. Unter den Befragten haben

- 65 Prozent ihren Rechner passwortgeschützt
- 63 Prozent ihr WLAN passwortgeschützt
- 61 Prozent ein Virenschutzprogramm installiert
- 49 Prozent ihren Dienst- und Privatrechner voneinander getrennt
- 41 Prozent ihre E-Mails und
- 38 Prozent ihre Datenübermittlung verschlüsselt.

Ähnlich viele, nämlich 37 Prozent, nutzen VPN-Verbindungen. Unter den Befragten verwenden 31 Prozent Cloud-Dienste zur Datensicherung. Mehr-Faktor-Authentifizierungen werden lediglich von 27 Prozent genutzt. Nur rund 12 Prozent der Umfrageteilnehmer verwenden keine der genannten Sicherheitsvorkehrungen.

Zum Artikel von All About Security

April 2020

Phishing mit Corona-Bezug nahm um 600 % zu

Die Corona-Krise bot auch Gelegenheit für so genannte Cyberkriminelle. Eine beliebte Methode stellte dabei „Phishing" dar, also das Abgreifen von sensiblen Daten über gefälschte Webseiten und E-Mails. Wie verbreitet diese Form der Cyberangriffe während der Pandemie war, zeigte eine Studie von knowbe4 eindrucksvoll.

Die Plattform für Security-Awareness-Training und Phishing-Simulationen stellte fest, dass Phishing-E-Mail-Angriffe im 1. Quartal 2020 um 600 Prozent zugenommen haben. In simulierten Phishing-Tests waren E-Mails mit der Aufforderung, das Passwort zu überprüfen, am erfolgreichsten. E-Mails mit Corona-Bezug folgten auf Platz zwei. Änderung der Urlaubs- und Krankheits-Richtlinien, Server-Updates, Warnungssysteme, Ankündigungen der Personalabteilung oder Hinzufügen zu Microsoft-Teams waren weitere Phishing-Anlässe.
Das Unternehmen untersuchte dafür Zehntausende E-Mail-Betreffzeilen aus Phishing-Simulationen, aber auch aus der Praxis.

Zum Artikel von Netzpalaver

Kommentar zum 1. Trimester 2020

„Unternehmen, die in den ersten Wochen der Pandemie Cloud Services nutzten, hatten einen großen wettbewerblichen Vorteil“

Timm Börgers, Managing Partner & Senior Trusted Advisor, verantwortet bei carmasec die Security-Technologieberatung.

Die Pandemie stellte Anfang des Jahres viele Unternehmen vor die Herausforderung die Arbeitsfähigkeit ihrer Mitarbeiter auch aus dem Home-Office sicherzustellen. Aufgrund einfacher Skalierbarkeit, schneller Inbetriebnahme und hoher Verfügbarkeit wurden Cloud Services im Eilverfahren eingeführt. Wer sich schon mit dem Thema Cloud auseinandergesetzt hatte, konnte von bereits erstellten Konzepten und gesammelter Erfahrung enorm profitieren.

Auch in den kommenden Jahren wird die Verlagerung von Geschäftsprozessen in die Cloud ein Thema sein. Dabei ist darauf zu achten, das generelle Sicherheitsniveau infolge von Home-Office oder Cloud Services nicht aufzuweichen. Vielmehr muss ein Weg gefunden werden, wie auch über die eigene Infrastruktur hinaus Informationen in angemessener Weise geschützt werden können.

Mai 2020

Nach Cyberangriff: Ruhr-Universität Bochum teils arbeitsunfähig

Zum Artikel von Forschung und Lehre

Nachrichten über so genannte Hackerangriffe liest man in den Medien immer häufiger. Welche Tragweite ein solcher Angriff haben kann, zeigte der Computerangriff auf die Ruhr-Universität Bochum. Der Angriff erfolgte mit einer Verschlüsselungssoftware. Die Folge: PC-Anwendungen in den Verwaltungen funktionierten nicht mehr, das interne Serviceportal der Universität konnte nicht mehr angesteuert werden und der Zugriff auf die E-Mail-Anwendung Outlook und den VPN-Tunnel waren nicht mehr möglich. Letzteres war besonders erheblich, weil es das Arbeiten und Studieren von zu Hause stark einschränkte.

Die Universitätsleitung reagierte sofort indem sie alle zentralen Server und Backup-Systeme herunter fuhr. Zudem beauftragte sie eine externe IT-Firma, die Schäden auszuwerten und Spuren bezüglich der Angreifer zu ermitteln. Studierende und Beschäftigte wurden sehr zeitnah benachrichtigt. Außerdem richtete die Universität eine Notfall-Website ein, um alle Betroffenen zu informieren.

Juni 2020

Weisenrat für Cyber-Sicherheit legt ersten Bericht vor

Zum Artikel von Behörden Spiegel

Eine Premiere in Deutschland: Zum ersten Mal hat ein Weisenrat für Cyber-Sicherheit der Bundesregierung seinen Bericht zu drängenden Themen der Informationssicherheit vorgelegt. Damit leiste er einen Beitrag zur Immunisierung der Gesellschaft gegen Cyber-Attacken, wird Dirk Backofen zitiert. Er ist Vorstandsvorsitzender des Cyber Security Clusters Bonn e.V., der den Weisenrat 2019 ins Leben gerufen hat. Um das Fundament für eine cyber-resiliente Wirtschaft und Gesellschaft in Deutschland zu legen, formulierte der Rat acht Empfehlungen:

- Technologie muss sich dem Menschen anpassen, um ihn zu entlasten und zu schützen
- Hersteller müssen sich zu regelmäßigen Schwachstellentests und Sicherheitsupdates verpflichten
- Digitale Prozesse und Infrastrukturen müssen angriffsresilienter werden
- Technologische Souveränität muss erhöht und bewahrt werden
- Digitale Infrastrukturen in smarten Städten müssen jederzeit verfügbar, verständlich und beherrschbar bleiben
- KI-Systeme müssen transparent und zertifizierbar sein
- Langlebige Produkte müssen kryptoagil gestaltet werden
- Der Schutz der Demokratie muss online verstärkt werden

Dem Weisenrat für Cyber-Sicherheit gehören 6 Professorinnen und Professoren aus Darmstadt, Bochum, München, Gelsenkirchen, Göttingen und Bonn an.

Juli 2020 (1)

Cyber Warfare: Wenn Krieg im Internet stattfindet

Konflikte werden nicht mehr nur physisch auf Schlachtfeldern ausgetragen. Sie finden auch im Cyberspace statt: Spionage, Sabotage und Social Engineering sind dabei nur einige Methoden, die zur Anwendung kommen. Diesem Thema hat die Konrad-Adenauer-Stiftung eine ganze Veranstaltungsreihe gewidmet: Unter „Kommunikation, Resilienz und Sicherheit" haben Experten der Bundeswehr und der saarländischen Landesregierung ihre Einschätzungen im Rahmen eines Online-Seminars vorgetragen. Ammar Alkassar, Chief Information Officer (CIO) der Regierung des Saarlandes formulierte vier Thesen:

1. Cybersicherheit wird zu einem wesentlichen Parameter geopolitischer Konflikte.
2. Es existieren noch keine Standard-Werkzeuge in der Cyber-Abwehr.
3. Künstliche Intelligenz wird ein Gamechanger in der Cybersicherheit.
4. Fähigkeiten zur Cyber-Abwehr werden kriegsentscheidend sein.

Zum Bericht der Konrad-Adenauer-Stiftung

Generalmajor Jürgen Setzer, Chief Information Security Officer der Bundeswehr (CISOBw), führte in seinem Impulsreferat an, dass die Bundeswehr auf diese Entwicklungen frühzeitig reagiert habe. Mit ihrer Organisationseinheit CIR, Cyber- und Informationsraum habe sie die Grundlage für den Aufbau notwendiger Fähigkeiten geschaffen. Alkassar und Setzer sind sich allerdings einig, dass diese Bedrohungen nur gesamtstaatlich, gesamtgesellschaftlich, national und international abgewehrt werden können.

Juli 2020 (2)

Studie des eco-Verbands zeigt: Cyber-Angriffe nehmen zu

Zum Artikel von datensicherheit

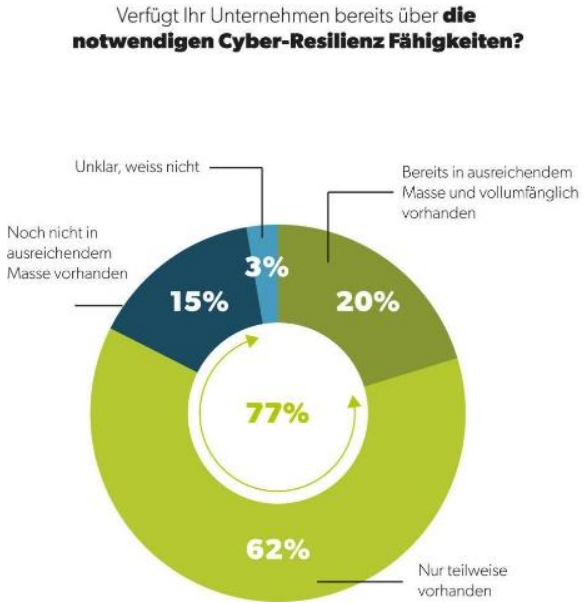
Unternehmen unterschätzen immer noch die Bedrohungslage. Zu dieser Erkenntnis gelangt der Verband der Internetwirtschaft eco in seiner IT-Sicherheitsstudie. „Die Diskrepanz bei der Beurteilung der eigenen Sicherheitslage und der Sicherheitslage in Deutschland allgemein zeigt, wie schwer es selbst Experten fällt, die Bedrohung richtig einzuschätzen“, sagt Oliver Dehning, Leiter der Kompetenzgruppe Sicherheit im eco. „Gerade viele Mittelständler stehen im Fokus international agierender Cybercrime-Netzwerke und sind sich dessen nicht bewusst.“

Cornelia Schildt, ebenfalls Sicherheitsexpertin bei eco, warnt, dass die Angriffe immer komplexer und vielfältiger werden. In jedem dritten Unternehmen (28 Prozent) hat es den Autoren der Studie zufolge mindestens einen gravierenden Sicherheitsvorfall gegeben. Dabei handelte es sich meist um Attacken durch Ransomware, Website Hacking oder DDos-Attacken. Aus Sicht des Verbands der Internetwirtschaft sind daher die drei wichtigsten Sicherheitsthemen: Verschlüsselung, Mitarbeiter-Sensibilisierung und Datenschutz. Wichtigste Vorsorgemaßnahme sind jedoch Notfallpläne. Rund 63 Prozent der Unternehmen haben hierzu vorgesorgt.

August 2020

Cyber-Resilienz wird zu Top-Priorität

88 Prozent der befragten Entscheider erachten Cyber-Resilienz als Top-Thema in der Cybersicherheit. 75 Prozent gaben an, dass ihr Budget dafür in den letzten zwei Jahren zugenommen hat. Dies ergab eine Studie der Schweizer Unternehmensberatung AWK Group. Dafür hat diese 100 Entscheider auf der Grundlage eines strukturierten Fragebogens befragt. Die größten Hürden Cyber-Resilienz im Unternehmen anzuwenden, sind den Befragten zufolge in erster Linie technischer Art.
Konkret nannten sie eine mangelhafte IT-Architektur und fehlende technische Fähigkeiten im eigenen Unternehmen, Anforderungen der Cyber-Resilienz zu erfüllen. Widerstände in der IT, fehlendes Top Management-Commitment oder Finanzierung stellen eher niedrige Hürden dar. Die Entscheider wurden darüber hinaus zur Rolle der Cybersicherheit befragt. Besonders erstaunt hat die Autoren der Studie, dass 70 Prozent der Befragten Cybersicherheit nicht nur als eine Voraussetzung für professionelles Handeln erachten. Sie bewerten sie vielmehr als Differenzierungsmerkmal am Markt. Sorge macht den Autoren allerdings, dass 54 Prozent der Entscheider zwar Kontinuitätsanforderungen definiert haben, diese allerdings im Ereignisfall nicht anwenden. Stattdessen improvisieren sie. Dabei sind die Fähigkeit zur Erholung nach einem Angriff und die Gewährleistung der Kontinuität wichtige Merkmale von Resilienz.



Zum Artikel von Forschung und Lehre

Kommentar zum 2. Trimester 2020

„Die Pandemie muss für alle Unternehmen ein Weckruf sein, Security-Projekte nicht weiterhin auf die lange Bank zu schieben!“

Jan Sudmeyer, Managing Partner & Senior Trusted Advisor, verantwortet bei carmasec das Security-Projektmanagement.

Die Entspannung der Corona Situation im Sommer bot Gelegenheit für ein erstes Zwischenfazit: Unternehmen, welche in der Vergangenheit bereits Digitalisierungsprojekte erfolgreich abgeschlossen hatten, konnten sich auf die Aufrechterhaltung ihres Geschäftsbetriebs aus dem Home-Office fokussieren.

Sie mussten dabei weniger, durch ad-hoc Maßnahmen bedingte, Kompromisse in Bezug auf Cybersicherheit machen. Dies ist insbesondere vor dem Hintergrund relevant, dass die Anzahl der (erfolgreichen) Cyberattacken im Frühjahr deutlich zugenommen hat. Dies muss ein Weckruf für alle Unternehmen sein, Security Projekte nicht weiterhin auf die lange Bank zu schieben.

September 2020

Das Digitalbarometer: Bürgerbefragung zur Cyber-Sicherheit

Zum Artikel von stern.de

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichte im September 2020 das „Digitalbarometer 2020 Bürgerbefragung zur Cyber-Sicherheit". Demzufolge ist jeder vierte Befragte Opfer von Kriminalität im Internet. Ein Drittel der Betroffenen (32 Prozent) hatte gar einen realen Schaden. Zu den häufigsten Straftaten zählen

- Betrug beim Online-Shopping (44 Prozent)
- Fremdzugriff auf einen Online-Account (30 Prozent)
- Phishing (17 Prozent) oder
- Schadsoftware wie Viren oder Trojaner (11 Prozent)

Die Befragten nutzen durchschnittlich mehr als vier Geräte. „Je mehr Geräte eine Person besitzt, desto höher ist die Wahrscheinlichkeit, dass sie bereits Opfer von Cyberkriminalität wurde", resümieren die Autoren von BSI.
Um sich zu schützen, nutzen die Befragten ein aktuelles Virenschutzprogramm (57 Prozent), sichere Passwörter (48 Prozent) und eine aktuelle Firewall (47 Prozent). „Diese Maßnahmen sind wichtig, reichen jedoch nicht aus," heißt es in der Studie. Insbesondere bei der Nutzung von privaten Geräten im Home-Office bieten Checklisten Hilfestellungen für den Ernstfall. Eine Präventionsmaßnahme, die auch das BSI empfiehlt.

Oktober 2020

Corona-Pandemie zwingt Finanzbranche zur Resilienz-Strategie

Zum Artikel von
gi Geldinstitute

Die Corona-Pandemie hat nahezu allen Branchen getroffen - so auch die Finanz- und Bankenbranche. Die Bedrohungslage, in der sie sich befindet, ist allerdings vielschichtig:

Zum einen hat sich das Kreditrisikoumfeld verschlechtert. Steigende Arbeitslosigkeit und schrumpfende Volkswirtschaften erschweren es Banken, die wachsenden Kreditrisiken einzudämmen. Aufgrund der Lehren der Finanzkrise in 2008 hat die Branche technische Frühwarnsysteme implementiert So wird mit Hilfe von Hochfrequenzanalysen großer Datenmengen schnell identifiziert, ob und warum ein Kreditnehmer in Zahlungsschwierigkeiten geraten könnte. Durch automatisierte Prozesse und Robot Process Automation, wie sie in Chatbots eingesetzt werden, sind Banken in der Lage, steigenden Arbeitsaufwand zu kompensieren.

Allerdings erschwert die Beschleunigung der Digitalisierung durch die Corona-Pandemie die Bedingungen. Besonders der Trend zum Homeoffice eröffnete Cyberkriminellen zahlreiche Schwachstellen. In Zusammenarbeit mit Regierungen, Aufsichtsbehörden und anderen Banken haben Finanzinstitute neue technologische Modelle zum Schutz des Finanzsystems entwickelt. Darunter die Echtzeitanalyse von Streaming-Daten mit Unterstützung durch Künstliche Intelligenz und Maschinelles Lernen. Es zeigt sich, auf beiden Ebenen der Bedrohungslagen, denen die Finanz- und Bankbranche ausgesetzt ist, müssen Finanzinstitute für ihre Cybersicherheit eine Resilienz-Strategie entwickeln.

November 2020

Gastbeitrag: Europa zum führenden Ort für Cybersicherheit machen

„Wir müssen Cybersicherheit als eine zentrale Gestaltungsaufgabe für die EU begreifen.“ Diese Forderung stellte Dr. Markus Richter in seinem Gastbeitrag für das Handelsblatt. Anlass war die Ankündigung der Europäischen Kommission, im Dezember eine neue „EU-Strategie für die Cybersicherheit“ vorzustellen. Richter ist IT-Beauftragter der Bundesregierung (CIO Bund) und Staatssekretär im Bundesinnenministerium. Als Leiter der IT-Abteilung des Bundesamts für Migration und Flüchtlinge (BAMF) hat er 2015 das Asylverfahren digitalisiert.

In seinem Artikel machte er auf die Gefahren aufmerksam. „Digitalisierung birgt aber auch erhebliche Risiken für unsere Sicherheit. IT-Ausfälle, Datendiebstähle und Betrug können unsere Sicherheit und unser aller Wohlergehen massiv beeinträchtigen. Diese Bedrohungen machen nicht an Grenzen halt.“ Entsprechend forderte er verstärkte Kooperation auf EU-Ebene und mit der EU, „um für künftige Cybervorfälle gerüstet zu sein!“

Dafür setze sich das Bundesministerium für die Errichtung eines europäischen Kompetenzzentrums Cybersicherheit ein“, so Richter. „Über dieses Kompetenzzentrum sollen in der kommenden EU-Finanzperiode 2021 bis 2027 gezielt Forschungsmittel eingesetzt und Anreize für private Investitionen in neue, europäische Cybersicherheitslösungen geschaffen werden.“ Gemeinsames Ziel sei es, die Innovationskraft und den Erfindergeist zu wecken und Europa als führenden Ort für Spitzentechnologie in der Cybersicherheit zu etablieren.

Zum Artikel des Handelsblatts

Dezember 2020

Cyberangriff auf den Impfstoff-Hoffnungsträger

Zum Artikel des Ärzteblatts

BNT162b2, so heißt das Objekt, auf das Cyberkriminelle bei ihrem Angriff auf die Europäische Arzneimittel-Agentur am 9. Dezember abgezielt haben. Besser bekannt ist es als der Covid-19-Impfstoff der Firmen BioNTech und Pfizer. Der Impfstoff hat volkswirtschaftlich enorm große Bedeutung.

Eine Schwachstelle bildete das IT-System der Behörden. So hatten die Angreifer Zugriff auf „einige Dokumente“ im Zusammenhang mit dem Zulassungsantrag, teilte die Europäische Arzneimittel-Agentur mit. Für die Aufklärung der Angelegemheit wurde Mikko Hyppönen von F-Secure eingeschaltet. Er gilt als einer der führenden Sicherheitsexperten weltweit. Hyppönen ist sich sicher, dass der Angriff nicht von gewöhnlichen Kriminellen, sondern im Auftrag eines Staates durchgeführt wurde. BioNTech selbst sei fähig gewesen, die eigenen Computersysteme zu schützen. „Es gibt jedoch nichts, was sie tun könnten, um ihre Forschungsdaten zu schützen, wenn diese im Rahmen der Genehmigungsverfahren auf IT-Systemen der Regierungen landen. Angreifer werden den einfachsten Weg finden, um Zugang zu den Daten zu erhalten, hinter denen sie her sind“, wird Hyppönen im Ärzteblatt zitiert.

Die Behörden-Chefin Emer Cooke versicherte, dass die Agentur „voll funktionsfähig“ sei. Weder sei der Zulassungsprozess unterbrochen noch sei die Auslieferung der Impfstoffe beeinträchtigt. Das genaue Ausmaß des Angriffs wird aktuell untersucht.

Kommentar zum 3. Trimester 2020

„Die Umsetzung eines professionellen IT-Risikomanagements und von Maßnahmen der Cybersicherheit erzeugen Wettbewerbs- und Produktivitätsvorteile.“

Carsten Marmulla, Managing Partner & Senior Trusted Advisor, verantwortet bei carmasec die Magementberatung zu IT-Governance, Risk & Compliance.

Die Krisensituation hat viele Unternehmen zu Ad-hoc-Maßnahmen gedrängt, um einen möglichst reibungslosen Geschäftsbetrieb fortführen zu können. Hieraus entstehen Chancen, um aus eigenen oder fremden Erfahrungswerten seine Digitalisierungsstrategie zu optimieren und ggf. schneller umzusetzen als zuvor geplant. Es locken Wettbewerbs- und Produktivitätsvorteile, sofern Anforderungen an ein professionelles IT-Risikomanagements und der Cybersicherheit berücksichtigt und in die Strategie integriert werden. Zudem lassen sich die Erkenntnisse zur Verbesserung des Business Continuity Managements nutzen, um gestärkt und widerstandsfähiger aus der Krise zu kommen.


Wir wünschen Ihnen Frohe Weihnachten und
einen guten Rutsch ins Jahr 2021.

Melden Sie sich für unseren Newsletter an: www.carmasec.com/newsletter

Hauptsitz:
carmasec GmbH & Co. KG
Ruhrallee 185
45136 Essen
Germany

Niederlassung:
carmasec GmbH & Co. KG
Im Mediapark 5
50670 Köln
Germany

Telefon: +49 (0) 201 426 385 900
Fax: +49 (0) 201 426 385 909
Web: www.carmasec.com
Email: contact@carmasec.com