Cyber Security 2020+
Was kommt auf uns zu?

Anfang Februar; bin ich nicht schon etwas zu spät dran, mich um Vorhersagen für 2020 zu kümmern? Zum Glück haben wir ja noch ein paar Tage Zeit in diesem Jahr, und zudem befinden wir uns heuer am Beginn einer neuen Dekade.

Alle Jahre wieder ein Blick in die Glaskugel, muss das wirklich sein? Ich denke schon. Warum ich das so sehe? Zwei gute Gründe:

Erstens empfinde ich den Cyber-Security-Blick-nach-Vorne erheblicher fundierter als das in vielen anderen Bereichen der Fall ist. Mit gesundem Menschenverstand werden die Erfahrungen des vergangenen Jahres extrapoliert. An dieser Stelle gleich ein Dank an die vielen Spezialisten und Unternehmen, die zu Beginn eines jeden neuen Jahres versuchen ihre Erfahrungen und Wissen zu einer Einschätzung zusammenfassen.

Zweitens ist der Übergang vom alten zum neuen Jahr immer eine gute Zeit, sich zumindest JETZT Gedanken zu machen und sich wenigstens einen guten „Vorsatz“ auf die Fahne zu schreiben und diesen dann hoffentlich auch umzusetzen. Natürlich ist es viel besser, Reviews kontinuierlich durchzuführen. Klar, dass uns auch dieses Jahr wieder überraschen wird mit neuen Angriffen, Bedrohungen, Kampagnen, mit denen wir so überhaupt nicht gerechnet haben. Es gilt die alte Weisheit: Eine gute Vorbereitung, Überdenken von Prozessen, Werkzeugen, Verfahren und Verhaltensregeln bereits im Vorfeld ist ein Muss für Informationssicherheit.

Für mich ist das Sichten der Vorhersagen vergleichbar mit guter Vorbereitung auf einen Zweikampf, wo man hofft als Sieger aus dem Ring zu steigen - und falls man doch niedergeschlagen wird, schnell wieder aufzustehen.

Ich möchte Ihnen in diesem kurzen Beitrag Prognosen für 2020 von einschlägigen Security Unternehmen zusammenfassen. Wenn dies Ihnen Ideen schenkt, was für ihr eigenes Unternehmen jetzt dran sein könnte, hat sich der Aufwand gelohnt. Wenn es also gut geht, werden Ihnen Bereiche

aufgezeigt, die Sie noch nicht genügend im Blick haben, wenn Sie überall gut unterwegs sind, umso besser.

Drei Teile erwarten Sie:

1. Wo stehen wir zu Beginn des neuen Jahrzehnts?
2. Was erwartet uns 2020?
3. Unser Fazit und welche Quellen wir berücksichtigt haben.

Vorab: Beim Durcharbeiten der Vorhersagen stieß ich irgendwann auch auf die Metaanalyse von Dan Lohrmann (Govtech) „Top 20 Security Predictions 2020“ (s. Kapitel 4). Diese ist sehr umfassend, gut zu lesen und unbedingt zu empfehlen, v.a. wenn Sie eine kurze Zusammenfassung der jeweiligen Vorhersage möchten. Darum werde ich dies nicht wiederholen, sondern beschränke mich auf eine Darstellung der durchgängigen Linien über alle Dokumente.

In wie weit dies objektiv oder meine subjektive Wahrnehmung widerspiegelt, müssen Sie selbst entscheiden? Auch ich habe meine Lieblingsthemen, wie auch jede Quelle eine Spezialmeinung hat und Schwerpunkte der jeweiligen Firma durchscheinen lässt. Für mich war das Lesen auf alle Fälle ein Gewinn.

Am Ende des Beitrags finden Sie eine Tabelle mit den Prognosen, die ich berücksichtigt habe und die überwiegend lesenswert sind.

1 Wo stehen wir?

Mitte Januar wurde der neue Allianz Risk Report 2020 veröffentlicht. Wie immer spannend, da er ja auch den Geldgebern ein wichtiger Indikator ist, wo investiert werden sollte. Cyber Security stieg zum weltweiten Toprisiko für Unternehmen auf - 2013 noch unter ferner liefen und nun weltweit auf Platz eins, in Deutschland auf Platz zwei. Cyberrisiken liefern zudem einen großen Beitrag zu dem anderen Toprisiko der Betriebsunterbrechung. Es werden mehr Schäden erwartet, mit steigender Schadenshöhe. Zudem erwartet die Allianz teure Datenschutzklagen in den kommenden Jahren.

Alle sind sich einig, dass Cyber Security in der letzten Dekade zum Topthema aufgestiegen ist und sicher das Topthema des neuen Jahrzehnts bleiben wird. Die „Einschläge“ kommen für jedes Unternehmen näher und nach wie vor gilt: Es ist keine Frage, ob es einen trifft, es ist die Frage wann, wie oft und wie man es merkt.

Das Thema Cyber Security sollte eigentlich doch durch sein. Hohe Awareness, gut ausgebildete Mitarbeiter, gute Vorbereitung auf einen Angriff, …. Dem ist leider nicht so. Bei unseren Kundengesprächen sehen wir teilweise noch immer eine große Naivität teilweise auch Ignoranz – im geschäftlichen sowie auch im persönlichen Bereich: „Meine Daten interessieren doch keinen.“ „Mir ist noch nie was passiert.“ Dies sind nach wie vor gängige Sätze. Insbesondere in kleineren Betrieben, Praxen, Vereinen und Gemeinnützigen Organisationen gilt noch immer das Prinzip „Augen zu und durch!“. Geld für IT-Sicherheit wird vorbeugend sehr vorsichtig eingesetzt, kommt es zum Vorfall spielen die Kosten dann keine Rolle mehr.

Security Awareness, der „Faktor“ Mensch also, ist nach wie vor ein zentrales Thema und Grundlage für gute Cyber Security. Noch immer gibt es kaum Verständnis, dass die eigenen Geräte für ein Botnetz missbraucht werden könnten, dass Bewegungsdaten auch wertvoll sind, dass bei

anonymisierten Daten heute durch künstliche Intelligenz (KI) der Personenbezug oftmals wiederhergestellt werden kann.

Auch in den kommenden Jahren steigt die Datenmenge enorm weiter. Daten werden mehr und mehr, komplexer, unübersichtlicher, aber zugleich immer besser auswertbar, dank Big Data und KI-Werkzeugen. Künftig werden Daten, insbesondere durch 5G von noch mehr Geräten mit größerer Bandbreite übertragen werden. Praktisch alle Geräte von der Glühbirne über das Handy bis zum Server müssen in Sicherheitsüberlegungen einfließen.

Security hat aufgerüstet. Ein Meilenstein war das Zusammenführen vieler Daten im SIEM-System, dieses wird nun durch KI-Funktionen angereichert und mit SOAR (Security Orchestration, Automation and Response) erweitert. Der Markt bietet ein breites Angebot an Cyber Security as a Service, die Erweiterung der Firewall mit IDS, IPS und DLP Werkzeugen und vielem mehr.

Leider führt dies alles nicht zur Entspannung. Man stellt eher eine steigende Anspannung in der Cyber Security fest und hat das Gefühl, die Unsicherheit wächst, aber es ist mehr ein dumpfes und dubioses Unwohlsein mit viele Fragen und komplizierten Antworten. Das liegt teilweise auch an neuen verteilten, offenen Architekturen, die man nicht mehr selbst in der Hand hat, auch an den Prozessen, die in die Jahre gekommen sind und hierfür nicht ausgelegt waren.

Für digitale Innovation stellt Cyber Security nach wie vor die Achillessehne dar. Neben der Datensicherheit ist zunehmend auch der Datenschutz ins Blickfeld gerückt. Dies wurde maßgeblich durch die Datenschutz Grundverordnung (DSGVO) befeuert.

Insbesondere in Europa zwingt der Gesetzgeber mit empfindlichen Strafen verstärkt zum Datenschutz, aber auch andere Länder ziehen nach, zum Beispiel ist Kalifornien in den USA der Vorreiter. Große Abmahnwellen blieben 2019 aus, es gab jedoch erste empfindliche Strafen: Deutsche Wohnen mit 14,5 Mio. €, 1&1 mit knapp 10 Mio. €, Google in Frankreich mit 50 Mio. € oder in Großbritannien die BA mit 200 Mio. €.

Die Angriffstaktiken haben sich verfeinert. Hier drei Beispiele:

1. Phishing entwickelte sich vom breit angelegten Angriff über das Spear-Phishing (gezielter Adressatenkreis) hin zu einem flexiblen Phishing, wo Angriffsbreite und gezielte Ansprache den Wünschen entsprechend einstellbar sind. Solch eine Entwicklung sehen wir zurzeit wieder bei der Ransomware, die sich vom breit angelegten Angriff zur Targeted Ransomware hin entwickelt und von der erwartet wird, dass sie sich im kommenden Jahr auf die Cloud hin erweitert.
2. Eine Entwicklung, die uns sicher weiter beschäftigen wird, ist Ausweitung des Angriffs über die volle Breite an Geräten, IIoT, Consumer IoT, PLC s (Programmable Logic Unit) für Maschinen-bzw. Anlagensteuerungen, Netzwerkkomponenten. Alles, was vernetzt ist, wird zum potenziellen Angreifer und bleibt ein mögliches Angriffsziel.
3. Angreifer beziehen mehr und mehr die gesamte Logistikkette mit ein. Ist man ein Unter-/ Lieferant oder Partner des eigentlichen Zielunternehmens, wird man automatisch selbst zum Ziel.

Standardisierte Prozesse haben in vielen Unternehmen Einzug gehalten, die ISO27k-Familie spielt hier nach wie vor die erste Geige, im deutschen Behördenumfeld besonders zudem der BSI Grundschutz. Risikomanagement oder Business Continuity Management, sind inzwischen eingeführt, oftmals jedoch nur rudimentär. Auch zur Risikoübertragung gibt es inzwischen eine große Vielfalt von Versicherungsangeboten.

Prinzipien wie „Security by Design" oder "Security by Default" werden zunehmend umgesetzt. Man merkt jedoch an der Güte mancher Implementierung, dass noch immer frühe Markteinführung bzw. „User Convenience" vorgeht. Der Markt wünscht sich „Security out of the Box" zum Nulltarif. Wir

sehen aber in allen Bereichen, dass dies nicht zu erreichen ist. Oftmals wird dann leider an der Ausbildung gespart, so dass Funktionen nicht oder falsch benutzt werden.

Trotz allem Wunsch nach Reduktion der Komplexität, sehen wir im Markt weiter eine starke Segmentierung, Best-In-Breed ist nach wie vor das gängige Muster, mit den bekannten Sicherheitsproblemen, v.a. an den Schnittstellen.

2 Was erwartet uns 2020?

2.1 Schwerpunkt Cloud

Cloud-Services werden verstärkt zum Angriffsziel. Die Cloud-First entwickelte sich in den vergangenen Jahren mehr und mehr zur Multi Cloud. Es gibt kaum mehr ein Unternehmen, das nicht Cloud Services auf vielfältige Weise nutzt. Cloud-Provider, allen voran Microsoft und Amazon sind bezüglich Cyber Security hervorragend aufgestellt. Der Sicherheitslevel, der hier inzwischen angeboten wird, kann von mittleren oder gar kleineren Unternehmen bei weitem nicht erreicht werden. Wo liegt aber dann die Herausforderung?

2.1.1 Unzureichende Beseitigung von Schwachstellen

Cloud Services von Unternehmen weisen in der Regel eine hohe Komplexität auf. Neue Funktionen werden rasch zur Verfügung gestellt und erfordert eine hohe Update-Rate. Das Unternehmen betreut oft hunderte von Containern, die gesplittet über viele virtuelle Maschinen auf Plattformen installiert sind und über unterschiedliche Schwachstellen verfügen. Dies bezieht sich auf die Technologie der Container, wie zum Beispiel Docker, runC, CRI-O, auf die Orchestrierung und auf die Bildumgebung. Dazu kommt der Einsatz vieler 3rd Party Produkte. All das erhöht die Komplexität der Gesamtlösung und die Häufigkeit notwendiger Sicherheits-Updates.

2.1.2 Problematische Konfiguration der Services

Aufgrund der Vielzahl an Funktionen sehen wir im Markt eine zunehmende Anzahl von unzureichend oder falsch konfigurierten Plattformen. Wie oben beschrieben, bieten die Cloud-Provider ein breites Instrumentarium für die IT-Sicherheit an, das jedoch zwingend richtig konfiguriert sein muss. Hierzu braucht es besondere Ausbildung der Mitarbeiter des jeweiligen Unternehmens. Oft werden „XYZ as a Service“ aber als Vereinfachung verwendet, um sich das Leben einfacher zu machen, und die Systeme werden nur rudimentär konfiguriert und überwacht. Somit besteht die Gefahr, dass sie über viele Schwachstellen verfügen.

2.1.3 Einsatz von Edge Computing

Durch die Zunahme der Datenmengen und teilweise unterschiedlichen Eigentümer der Daten findet in vielen Services zunehmend eine erste Datenaggregierung vor Ort statt. EDGE Devices werden eingesetzt. Dies sind neue Kernkomponenten, die es besonders zu schützen gilt. Wir

sprechen hier von Geräten vom Typ Alexa Chromecast und „Konsorten“, insbesondere aber auch von zunehmend komplexeren Geräten, die eine erhebliche Datenmengen von vielen Endgeräten bearbeiten. Das Edge Computing wird in den kommenden Jahren an Bedeutung zunehmen, gerade hier muss ein hoher Sicherheitsstandard eingeführt sein und aufrechterhalten werden.

2.1.4 Zugriff auf die Services durch unterschiedlichste Geräte

Die Zeiten, in denen ausschließlich PCs, Tablets und Mobile Phones auf Services zugriffen haben, sind Historie. Zunehmend melden sich Maschinensteuerungen, Geräte wie Webcams, Mikrofone, Kleinststeuerungen, Kameras, Fernseher, Hausgeräte usw. an die Services an. Diese verfügen meist nur über einen unzureichenden bzw. gar keinen Schutz und haben ein hohes Infektionsrisiko. Damit steigt die Gefahr einer Infektion der Services stark an.

Zusammenfassend: Für das kommende Jahr erwarten wir eine stark steigende Anzahl der Angriffe auf Cloud Plattformen und Cloud Services, auch durch Ransomware, die Cloud Services bislang verschont hat.

2.2 Schwerpunkt 5G

2.2.1 Neue Technologie

Neuartige Technologien haben erfahrungsgemäß immer etliche (ungeplante) Schwachstellen. 5G Umgebungen sind Software-definierte Netzwerke, die beste Konnektivität mit hoher Bandbreite und niedrigerer Latenzzeit vereinen. Faktisch handelt es sich um viele gut vernetzte Minirechenzentren. Dies führt zu einer hervorragenden Erreichbarkeit, die natürlich auch Gefahren in sich birgt. So können z.B. in kurzer Zeit enorm viele Daten abfließen. Das Verhindern von unbeabsichtigtem Datenabfluss gewinn eine neue Dynamik.

Die komplexe Architektur bietet verglichen mit 4G zusätzliche Angriffsziele. Die Furcht vor einer unentdeckter „tödlicher“ Schwachstelle, einem sogenannten „Kill-Switch“ mag nicht ganz unbegründet sein.

2.2.2 Schnelle Durchdringung

Aktuell stellen wir eine verzögerte 5G Einführung fest. Dies aufgrund einer gewissen Skepsis in der Gesellschaft, die sich auf die politische Unterstützung auswirkt. Spürbar wird dies zum Beispiel bei der Genehmigung von Mobilfunk-Masten. Ist die Infrastruktur erst einmal da, wird die Nutzung sprunghaft erfolgen.

Es wird ein enormes Wachstum in der Heim-Vernetzung erwartet, und sogar noch mehr im Gesundheitswesen. Gerade dieses hantiert mit personenbezogenen, sehr sensiblen Daten, die einen hohen Profilwert haben (für die aktive Werbung bis hin zur Erpressung). Sowohl die eingesetzten Endgeräte als auch oftmals die eingesetzte Software verfügt über eine hohe Anzahl von Schwachstellen. Besonders gilt dies für Geräte im eigenen Heim, wo Geräte nach Aussehen und Preis gekauft werden und die Sicherheit noch immer kein wichtiges Kaufargument ist.

2.2.3 Hohe Konnektivität

Die gute Konnektivität von 5G haben wir bereits erwähnt. Kritisch beäugt wird u.a. das automatische Hand-Over zwischen WLAN und 5G (Hotspot 2.0 Funktionalität). Diese Schnittstelle wird gerade von unterschiedlichen Stellen intensiv untersucht.

Zusammenfassend: Durch die hohe Komplexität, die extreme Leistungsführung und die erwartet schnelle Durchdringung stellt die 5G Vernetzung ein sehr attraktives Ziel für Cyber Angriffe dar. Schutz vor Datenabfluss (DLP) gewinnt weiter an Bedeutung.

2.3 KI gewinnt weiter an Bedeutung

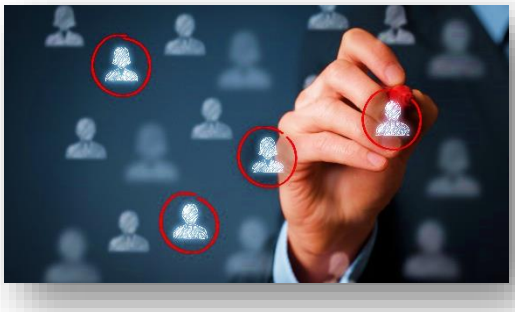
Im vergangenen Jahr sahen wir im großen Stil den Einsatz von KI bei der Cyber Security. Klar ist, dass wir hier ein janusköpfiges Thema vor uns haben. Zum einen hilft uns KI, Bedrohungen zu erkennen und Angriffe zu verhindern bzw. zu bekämpfen, auf der anderen Seite werden die Bedrohungen durch den Einsatz von KI-Algorithmen natürlich auch immer cleverer. Angreifer werden die KI im kommenden Jahr auf alle Fälle weiter verstärkt nutzen und mit hoher Kreativität neuartige Werkzeuge entwickeln.

Ein besonderes Augenmerk sollten wir den Deep-Fakes widmen. Inzwischen erleben wir durch KI in Echtzeit generierte Stimmen, die der jeweiligen Originalstimme täuschend ähnlich ist, auch durch KI veränderte Bilder und Videos in Echtzeit. Zurzeit werden diese Technologien verwendet um bestimmt Personen, wie wichtige Entscheider zu simulieren. Dies gibt BEC-Angriffen (Business E-Mail Compromise) eine komplette neue Dynamik. Wo man sich früher weitgehend auf Sprache oder Video verlassen konnte, ist es künftig nicht mehr möglich.

Da Ton und Video zum Beispiel auch bei der Authentifizierung Verwendung finden, werden hier überarbeitete Methoden und Prozesse nötig.

Neben dem Einsatz bei Deep-Fakes werden wir KI-Methoden in der Objektidentifikation und in der verstärkten Verknüpfung von Bewegungs- und Inhaltsdaten erleben. Anonymisierung von personenbezogenen Daten wird künftig durch intelligente Verknüpfungen im großen Stil ausgehebelt.

2.4 Zero Trust Network



Die von maßgeblichen Analysten promotete Abkehr von klassischen „perimetergeschützten“ Netzwerken hin zu einer Zero Trust Architektur, wie z. B. SDP (Software Defined Perimeter) wird in den kommenden Jahren erheblich an Bedeutung gewinnen. Neue Services werden in Koexistenz zu bestehenden Architekturen mit Zero Trust Architektur implementiert werden. Die zunehmende Mikrosegmentierung und die permanente Authentifizierung ist inzwischen gut instrumentalisiert und birgt einen erheblichen sicheren Sicherheitsgewinn.

Die Vorteile liegen auf der Hand, Rechte werden nicht mehr vom Zugang zum Netzwerk gesteuert, sondern permanent, service-, orts-, gerätespezifisch gewährt und überwacht. Segmentieren, isolieren und kontrollieren Sie Ihr Netzwerk. Drei Kernelemente sind:

- Geräte Authentifizierung
- identitätsbasierter Zugang und zugriffsorientierte Authentifizierung
- dynamisch bereitgestellte Konnektivität.

Da diese Technologie kein prinzipielles Drinnen oder Draußen kennt, sondern nur ein „Berechtigt in diesem Kontext“ eignet sie sich hervorragend auch zur Steuerung von offenen Netzen und für mobile Mitarbeiter. Daher erwarten wir einen verstärkten Einsatz bereits im kommenden Jahr.

Falls diese Technology neu für sie ist, finden Sie einen guten Einstiegsartikel zum Beispiel unter https://www.computerwoche.de/a/zero-trust-verstehen-und-umsetzen,3547307.

2.5 Sicherheitsprozesse

An der Prozessseite herrscht noch immer ein erhebliches Defizit. Während technische Maßnahmen inzwischen ein fester Bestandteil der IT-Planung sind, sind gelebte und trainierte Prozesse nach wie vor Mangelware. Doch gerade bei dem Vorfall, kommt man in einen Ausnahmezustand, in dem nur eine gute Vorbereitung richtiges Handeln erlaubt.

Die Prozesskette erweitert sich. Letztlich wird jeder Prozess-Schritt zum potenziellen Ziel. Die komplette Logistikkette wird angegriffen. Auch wenn das Unternehmen nicht das primäre Ziel ist, werde ich als Zulieferer, Kunden oder Partner automatisch selbst zum Ziel. Dies alles ist rekursiv und wiederholt sich für alle Subunternehmer. Eine durchgängige Sicherheitskette ist gefragt. Dies betrifft Skills, Kapazität und Kontinuität. Mitarbeiter müssen ausgebildet und das Wissen stetig aktualisiert werden. Wo bekomme ich ausreichende und vor allem die richtigen Kapazitäten für diese Spezialthemen? Gibt es Cyber Security Prozesse die Kontinuität ermöglichen? Dies sind nur drei Fragen, die uns im kommenden Jahr verstärkt beschäftigen werden.

Dies alles wird befeuert durch die zu erwartenden Datenexplosion mit 5G. Schon durch 5G werden wir zudem neue Businessmodelle erleben. Umso wichtiger sind gut funktionierende Sicherheitsprozesse und ein funktioniertes Risikomanagement (was passiert, wenn …). Da dies alles im Vorfeld nicht oder nur sehr schwer planbar ist, werden agile Prozesse nun auch in der IT Sicherheit ankommen. Ein Lernen aus anderen Bereichen ist unumgänglich. So werden CSOs/CISOs zunehmend von der SecDevOps Sichtweise lernen müssen.

Unterstützungsleistungen für die Nutzung von Cyber Security Standards wie die ISO 27k, BSI Grundschutz, MITRE oder ATT&CK Framework werden verstärkt nachgefragt werden.

2.6 Der „Faktor“ Mensch

Sicherheit wird nur gewährleistet werden können durch eine gute Ausbildung der Mitarbeiter und einfach zu benutzenden Instrumentarien.

Noch immer wird die Wichtigkeit einer kontinuierlichen Schulung unterschätzt. Dies gilt für die Sensibilisierung im Umgang mit Primärdaten, Bewegungsdaten und Geräten. Die Veränderung in der Arbeitsplatzgestaltung sowie die oben beschriebenen Herausforderungen der Digitalisierung sind nur mit Mitarbeitern gangbar, die ein ausreichendes Verständnis für Cyber Security haben. Die Notwendigkeit einer besseren Ausbildung ALLER Mitarbeiter nimmt weiter zu.

Ein zusätzlicher Grund ist die Nutzung einer Vielzahl an Geräten bei mobilem Arbeiten unterwegs und von zu Hause aus. In den dabei genutzten Netzwerken wimmelt es von unbekannten und teilweise sehr schlecht geschützten Geräten. Was für Gefahren muss ich dabei beachten und wie verhalte ich mich richtig?

Wie im Abschnitt „KI“ gezeigt, zwingen zum Beispiel Deep-Fakes zu einer kompletten Änderung im Agieren in Genehmigungsprozessen. Wir werden neue Dimensionen des Social Engineerings erleben. Phishing-Angriffe werden nach wie vor ein Thema bleiben und sich generell auf Kollaboration im Netz ausbreiten. Bewährte Technologien, wie zum Beispiel Double-Opt-In, werden zu Angriffszwecken missbraucht. Ich erwarte ein E-Mail und bestätige diese automatisch, ohne groß nachzudenken.

Multifaktor Authentifizierung wird zum Standard werden. Nach wie vor ist Benutzername und Passwort das wichtigste Authentifizierungsmerkmal. Um bei der Vielzahl an Verfahren den Anforderungen an Account und Passwörtern Rechnung tragen zu können, werden viele Unternehmen Passwortmanager einsetzen. Biometrie wird sich nur in Teilbereichen durchsetzen.

Der Datenschutz wird weltweit an Bedeutung zunehmen. GDPR wird auch in anderen Ländern angewendet werden und Bewegungsdaten werden zunehmend in den Fokus der Benutzer und des Gesetzgebers kommen.

3 Fazit

Es wird wieder ein spannendes Jahr(zehnt). Das Hin und Her von Angriff und Verteidigung wird bestimmt nicht abebben. Wir erwarten völlig neue Angriffsmethoden bzw. starke Verfeinerung bewährter Methoden durch den Einsatz von KI. Dies wird alle Wirtschaftsbereiche treffen und bestimmt auch von der Heimvernetzung nicht Halt machen.

Neben allen technischen Maßnahmen ist das zentrale Thema die Ausbildung aller Beteiligter. Ein Grundverständnis muss bei jedem vorhanden sein. Unternehmen sollten alle Mitarbeiter aktiv und aufgabenspezifisch trainieren. Webschulungen halten wir für eine gute Ergänzung, aber alleine nicht ausreichend. IT-Personal sollte den Ernstfall proben und stetig weitergebildet werden, Geschäftsführer sollten die IT-Sicherheit aktiv propagieren. Wichtig sind selbstverständlich gut ausgebildete Fachkräfte, denn hier herrscht schon seit längerem ein Mangel, der sich im kommenden Jahr weiter verstärken wir.

Kunden, Partner, Lieferanten werden künftig wesentlich stärker zusammenarbeiten müssen, um ausreichende Sicherheit in die gemeinsamen Prozesse zu bekommen.

Neben der Technik und den Menschen sind auch die gelebten Prozesse das dritte Standbein damit die Security stabil und sicher steht. Definieren, leben, prüfen und verbessern Sie Ihre Prozesse zur Datensicherheit und für den Datenschutz stetig.

Wir die secobit helfen Ihnen gerne dabei. Nehmen Sie Kontakt auf über info@secobit.de .

4 Diese Quellen haben wir berücksichtigt

Alle Artikel haben einen eigenen Reiz und Schwerpunkt. Unsere Empfehlungen sind:

- Watchguard oder Trendmicro als Einstieg. Watchguard, für den, er es kurz und bildhaft mag; Trendmicro stellt die Themen verständlich und optisch gut dar.
- Govtech gibt eine gute Zusammenfassung von 20 Quellen.

Autor	Link	Umfang
PaloAlto Networks	https://www.it-business.de/palo-alto-wie-it-security-die-welt-beeinflusst-a-893278/	Überblick in 9 Kapiteln, 4 S. Fokus auf EMEA
Fireeye	https://www.fireeye.com/current-threats/annual-threat-report/cyber-security-predictions.html	Fünf Themen auf 15 Seiten Beiträge von 5 Fireeye VPs
Forbes	https://www.forbes.com/sites/gilpress/2019/12/12/42-more-cybersecurity-predictions-for-2020/#45f3d4714a56 https://www.forbes.com/sites/gilpress/2019/12/03/141-cybersecurity-predictions-for-2020/#5b9551881bc5	Statements 141 + 42 Cyber Sec. Entscheider Sehr breites Themenfeld
Forcepoint	50 min Video https://www.brighttalk.com/webcast/15527/378881/2020-cybersecurity-predictions BLOG https://www.forcepoint.com/blog/x-labs/2020-forcepoint-cybersecurity-predictions	5 Themen Mit Video gut erklärt
Forrester	https://www.forrester.com/report/Predictions+2020+Cybersecurity/-/E-RES158258?docid=158258	Analyst muss bezahlt werden
Fujitsu	https://www.fujitsu.com/emeia/services/security/insights/security-prediction-2020/	12 Themen auf 4 Seiten Kurz und knackig
Gartner	https://e27.co/10-data-security-predictions-by-gartner-for-the-year-2020-20190826/	Analyst muss bezahlt werden
★ Govtech	https://www.govtech.com/blogs/lohrmann-on-cybersecurity/the-top-20-security-predictions-for-2020.html	Zusammenfassung von 20 Vorhersagen; guter Überblick
IDC	https://www.idc.com/getdoc.jsp?containerId=US45582219	Analyst muss bezahlt werden
Kaspersky	https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2019/11/20151759/KSB2019_APT-predictions-2020_web.pdf; Weitere 2020 Reports https://securelist.com/ksb-2019/	8 Kapitel Advanced Threats auf 5 Seiten Gute weitere Reports
McAfee	https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-labs-2020-threats-predictions-report/ Dataschutz: https://www.mcafee.com/blogs/consumer/consumer-threat-notices/data-privacy-predictions-2020/	5 Vorhersagen gut erklärt Eigener Datenschutz Report
RSA	https://www.rsa.com/content/dam/en/e-book/20-predictions-for-2020.pdf	20 Vorhersagen Jeweils 1-2 Sätze Erklärung
Sophos	https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophoslabs-uncut-2020-threat-report.pdf	7 Themen, 25 Inhaltsseiten Jeweils 3-4 Unterthemen
Splunk	https://www.splunk.com/pdfs/ebooks/security-predictions-2020.pdf	4 Kapitel auf 5 Seiten Gut erklärt
★ Trendmicro / BeyondTrust	https://documents.trendmicro.com/assets/rpt/rpt-the-new-norm-trend-micro-security-predictions-for-2020.pdf Deutsch: https://www.trendmicro.com/vinfo/de/security/research-and-analysis/predictions/2020	Überblick in 5 Kapiteln auf 21 Inhaltsseiten Sehr umfassend
Verizon	https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf	Databreach Report Mitte 2019
★ Watchguard	https://www.watchguard.com/de/wgrd-resource-center/predictions-2020	Kurzer Überblick in 7 Kapiteln Mit prima Kurzvideos

Anmerkung: Analystenquellen wurden zur Vollständigkeit aufgelistet. Die Informationen sind kostenpflichtig und wurden nur soweit berücksichtigt, wie frei verfügbar.

Schlussbemerkung

Das vorliegende Dokument wurde nach bestem Wissen und Gewissen erstellt. Sollten sich Fehler oder Ungereimtheiten eingeschlichen haben, bitten wir um Benachrichtigung. Auch sonst freuen wir uns über eine Rückmeldung an info@secobit.de.

Warenzeichen

Microsoft ist eingetragenes Warenzeichen der Microsoft Corporation. Alle anderen genannten Warenzeichen sind Eigentum ihrer jeweiligen Besitzer.

Copyright