Krisen-Management – Schutz durch Digitalisierung

INTELLIGENTE UNTERNEHMEN SIND DIE ZUKUNFT – Eine bessere Steilvorlage hätte die zweite Auflage des PLATOW UnternehmerFORUM kaum bekommen können. Nur zwei Tage vorher bemängelte das **Bundesamt für Sicherheit in der Informationstechnik** in seinem Lagebericht die IT-Sicherheit in Deutschland. Hat doch die Corona-Pandemie durch das verstärkte Homeoffice die Gefahrenlage durch Cyber-Kriminalität deutlich erhöht. Diese Erfahrung mit Unternehmen macht regelmäßig auch **Klaus-Peter Spieler,** Bereichsleiter der noch jungen **Cyber Security GmbH,** einer Tochter der Wirtschaftsprüfungsgesellschaft **BDO,** der die virtuelle Konferenz mit ausgewiesener Fachexpertise moderierte.

Klaus-Peter Spieler, BDO Cyber Security

BDO hat hierzulande ein Security Operation Center aufgebaut (s. Interview S. 7). Die dafür in mehreren Ländern erprobte Technologie kommt von einem israelischen Partnerunternehmen aus dem globalen BDO-Netzwerk, das führend im Bereich Cyber-Security ist. Einen Blick in die internen Kontrollsysteme lieferte der israelische BDO-Partner und Geschäftsführer **Ophir Zilbinger,** der aus Tel Aviv zugeschaltet war. Für den Cyber-Experten ist für eine effiziente Abwehr von Cyber-Angriffen eine Zusammenarbeit mit Geheimdiensten unabdingbar, in Deutschland jedoch aufgrund von Datenschutz und Compliance kaum durchsetzbar.

Rouven Morato, SAP SE

Auf den Boden der Realität gebracht hat die Tagungsteilnehmer **Rouven Morato** in seiner Keynote. Der Senior Vice President und General Manager von **SAP SE** machte deutlich, dass jeder in den vergangenen Monaten „schmerzhaft" vor Augen geführt bekommen habe, was so eine Krise eigentlich mit sich bringt. Für die Unternehmen gehe es auf einen Schlag nicht mehr darum, die nächste Marktchance zu nutzen oder langfristig erfolgreich zu bleiben. „Es ging nur noch ums schlichte Überleben", so die klaren Worte des SAP-Managers. So bezeichnete Morato denn auch die Krise als „Wake-up Call" für eine noch bessere Digitalisierung. Die Krise hat die Schwächen der Unternehmen aufgezeigt. „Auch bei SAP", gibt Morato selbstkritisch zu. Sogar das stark digitalisierte **DAX**-Unternehmen war „auf so viel" Homeoffice nicht vorbereitet. Die Krise hat aber auch Gewinner hervorgebracht. Doch nicht jedes Unternehmen kann zum eCommerce-Hotspot werden. Um zu den „intelligenten Unternehmen" zu gehören, sollten die Verantwortlichen nach Moratos Ansicht einige wichtige Kriterien beachten. Neben einem hohen Grad an Automatisierung und Transparenz sei auch eine hohe Profitabilität, basierend auf einer starken Agilität, eine Voraussetzung dafür. Dies führe letztlich zu einer hohen Resilienz und der Möglichkeit, in Krisen erfolgreich zu wirtschaften. Intelligente Unternehmen sind in der Lage, Daten, Systeme und Prozesse zu digitalisieren und dabei den Faktor Mensch einzubeziehen. „Digitalisierung ist kein IT-Projekt", betont der SAP-Fachmann. Wenn nur Software eingekauft würde, könne kein Digitalisierungsprojekt erfolgreich verlaufen. ■

Warum eine gefüllte „Kriegskasse" für Unternehmen wichtig ist

ABSCHIRMUNG DES GESELLSCHAFTERKAPITALS – Als Privatbank ohne klassisches Kreditgeschäft steht die Hamburger **M.M. Warburg & CO** sicherlich nicht exemplarisch für das, was der hiesigen Bankenlandschaft mit Blick auf die Pandemie und die in den Kreditbüchern möglicherweise schlummernden Risiken droht. Dennoch erkennt **Philip Marx,** Leiter Corporate Banking, dass schwelende Konflikte und Probleme im Mittelstand durch die Pandemie eine Art Nachbrenner erfahren haben. Viele Herausforderungen müssten jetzt „unausweichlich" angegangen werden, so Experte Marx, der als Bank u. a. kleinere Mittelständler in Sondersituationen begleitet. Im Vordergrund stehen dabei in der Regel Akquisitionsfinanzierungen, Eigenkapitalvorfinanzierungen, Refinanzierungen und Zwischenfinanzierungen.

Philip Marx, M.M. Warburg

Als Beispiel nennt der Unternehmenskenner fünf Fallstudien aus den Bereichen Lebensmittelindustrie, Automobilzulieferer, Immobilienentwicklung, Einzelhandel und Multimedia Agentur. In Zeiten wie diesen wird die Liquidität in den Unternehmen knapp. Banken fordern in der Regel Nachschüsse von Gesellschaftern. „Banker haben aber die unangenehme Eigenschaft, wenn ein Kapitalgeber einmal Geld reingegeben hat, dann setzen sie sich drauf und die Gesellschafter sehen das Geld meistens nicht wieder", so Marx. Hier gehe es also auch um die Frage, wie es gelingen kann, Nachschüs- ▶

se und Gesellschaftereinschüsse abzuschirmen. Gleichzeitig gibt es auch Auseinandersetzungen der Gesellschafter, wo es der Verhandlung dient, wenn nicht unbedingt klar ist, dass man mit seinem Erzfeind verhandelt. Hier kann man durch Abschirmungsstrategien durchaus Konfliktpotenzial minimieren. Unterdessen sind für M.M. Warburg Nachfolgelösungen in Familienunternehmen immer schwierig. Gerade dann, wenn über die Jahre eine solche Nachfolgelösung gewachsen ist und plötzlich auf der Zielgeraden durch Corona vereitelt wird. „Das ist tragisch, muss aber gelöst werden", sagt Marx, auch im Interesse der Gesellschaft, wenn kein Familienmitglied in die Nachfolge tritt, sondern es zu einem Exit kommen und Familienvermögen abgeschirmt werden soll. ■

Reputationsrisiken aus dem Netz minimieren und absichern

COOKIES-BANNER ALS GEFAHRENQUELLE — Unverzichtbar bei so vielen Risiken in Privathaushalten und Unternehmen sind Versicherungspolicen. An ihnen führt oftmals kein Weg vorbei. Die Assekuranz reagiert zunehmend in ihrer Produktpalette auf die Veränderungen durch die Digitalisierung, die durch Corona schlagartig an Tempo gewonnen hat. Arbeitsabläufe werden digitaler denn je. Das hat auch eine aktuelle Umfrage der Versicherungsgesellschaft **Arag** ergeben. Danach halten 64% der befragten Unternehmen mehr virtuelle Konferenzen ab. Umgekehrt vermuten 58% der Unternehmen, dass langfristig weniger Vorort-Meetings stattfinden. In diesem Zusammenhang steigt auch die Relevanz von Homeoffice und E-Learning. Umso wichtiger wird der Schutz, sich und sein Unternehmen rechtlich im Netz abzusichern. „Von der Unternehmensgenetik her fühlen wir uns als Rechtsschutzversicherer dazu aufgerufen, dem Kunden auf diesem Gebiet eine vernünftige Absicherung zu bieten", sagt **Frank Küper,** der bei der Düsseldorfer Arag den Stammvertrieb leitet. Damit ist er für über 1000 Vertriebspartner sowie über 100 Hauptgeschäftsstellen in Deutschland zuständig.

Frank Küper, Arag

Für ein sehr wichtiges Thema hält Vertriebsexperte Küper das Thema Datenschutz, das hierzulande durch die DSGVO geregelt ist. „Hier drohen auch Gefahren", berichtet Küper aus der Praxis. In den vergangenen Tagen und Wochen hat die Arag eine Vielzahl an Abmahnungen bei ihren Kunden erlebt. Anwälte und Abmahnvereine durchforsten vermehrt Webseiten und prüfen, ob die Bannerschaltung zum Thema Cookies rechtens ist. Die DSGVO und die Datenschutzrichtlinie für elektronische Kommunikation (ePR) geben vor, wie Unternehmen als Website-Eigentümer die Zustimmung ihrer Besucher aus der EU zu Cookies einholen und speichern müssen. Eine nicht konforme Cookie-Nutzung kann unter Umständen bis zu 20 Mio. Euro Strafe kosten. Schnell kann daraus ein juristisches Problem entstehen, worauf nicht jedes Unternehmen vorbereitet ist.

Image-Verlust durch schlechte Rezension

Ein weiteres Problem der Digitalisierung ist die Reputation im Netz. Rezensionen sind mittlerweile ein wichtiger Teil neben der professionellen Website als Visitenkarte eines Unternehmens. Erfahrungsberichte aus dem Internet gewinnen an Bedeutung. Es geht um die Frage, wie werden Unternehmen im Netz gesehen und bewertet. Leider sind dort auch Menschen unterwegs, die einem nur Schaden zufügen wollen. Im Netz ist es sehr einfach, etwa durch einen Flashmob oder schlechte Bewertungen wirtschaftliche Nachteile auszulösen. „Dieses Risiko hat in den vergangenen drei bis fünf Jahren extrem zugenommen", sagt Arag-Experte Küper. Hier seien Privatkunden und Firmen oftmals überfordert, was zugleich die dunkle Seite der Digitalisierung spiegelt.

Als einer der wenigen Versicherungsgesellschaften versucht die Arag als Smart Insurer schon seit 2013, mit den Inhalten der Produktreihe web@aktiv3.0 bei Kunden zu punkten. Bislang gelingt ihr das überwiegend bei Privatkunden. Die zunehmende Sensibilisierung für Reputations- und Rechtsrisiken aus dem Netz dürfte schon bald auch mehr Firmenkunden ins Boot holen. Als nützliche Tools haben sich bspw. der Reputations-Check, Rechtsschutz zu DSGVO-Themen oder das Online-Monitoring gezeigt. ■

IT-Compliance – Schutzschild vor Cyber-Gefahren

EIN NOTFALLHANDBUCH HILFT — Wie ein roter Faden zogen sich die Aussagen zu den gestiegenen IT-Risiken aufgrund der forcierten Digitalisierung durch fast alle Präsentationen, somit auch durch die Vorträge der Vertreter der Mannheimer Wirtschaftskanzlei **SZA Schilling Zutt & Anschütz.** Die Partner hoben die Notwendigkeit einer umfassenden IT-Compliance als Schutzschild zur Abwehr von Cyber-Kriminalität hervor. Was das konkret im Rahmen der Prävention bedeutet, erläuterte Experte **Horst Amannt,** der den Faktor Mensch als schwächstes Glied in der Kette wirksamer Prävention in den Mittelpunkt stellte.

Am Anfang des Präventionsprozesses stehen zunächst grundlegende Maßnahmen die IT-Infrastruktur betreffend, also der Hard- und Software. In einer IT-Sicherheitsrichtlinie werden der Umgang mit vertraulichen Informationen am Arbeitsplatz sowie der Zugang zu Büroräumen (z. B. Zugangskarten, Alarmsicherung) geregelt. Dazu gehört auch die Ausarbeitung eines IT-Notfallhandbuchs. Bezüglich der in der IT verwendeten Daten hält Jurist Amannt die Ausarbeitung einer internen Datenschutzrichtlinie für wichtig. Schließ-

lich runden regelmäßige Mitarbeiterschulungen zum Thema Datenschutz die Prävention ab. Erste Sofortmaßnahmen bei einem IT-Sicherheitsvorfall gehören zu einer effizienten und angemessenen Reaktion. An dieser Stelle kommt das Notfallhandbuch zum Einsatz, das elektronisch und in Papierform an verschiedenen Standorten, auf den Servern im Unternehmen, aber auch privat zuhause bereitzustellen ist. Zu den wesentlichen Inhalten des Notfallhandbuchs gehören die richtigen Ansprechpartner, der Kommunikationsplan, Pläne zum Aufbau der IT-Infrastruktur sowie Pläne für Sofortmaßnahmen und zur Einrichtung eines Notfallbetriebs. Zum Notfallhandbuch gehören aber auch Pläne zur Wiederherstellung des Normalbetriebs, wie sie ergänzend **EY-**Experte **Bodo Meseke** (s. S. 4) in seinem Vortrag beschreibt. ■

„Hacker sind kreativ und anpassungsfähig“

BDO baut ein Service Operation Center in Deutschland. Die Echtzeitüberwachung der Kunden-Netzwerke steht im Mittelpunkt. Darüber sprachen wir mit Klaus-Peter Spieler, Bereichsleiter Cyber Security.

Viele Unternehmen sind durch die Umstellung aufs Homeoffice gezwungen, kurzfristig Infrastruktur und Prozesse zur Verfügung zu stellen. Was müssen sie beachten?

Die Einrichtung muss festgelegten Bedingungen entsprechen – etwa, was den Zugang zu Rechner, Unterlagen und anderen Arbeitsmitteln angeht oder, je nach Vertraulichkeitsgrad, was ungestörte Kommunikationsmöglichkeiten betrifft. Dafür gibt es Checklisten. Generell müssen die Daten sicher sein und die EU-DSGVO eingehalten werden.

Im Frühjahr haben Sie zunehmende Phishing-Angriffe beobachtet, welche sich zum Teil auch auf Corona-Themen bezogen haben. Wie ist die Lage aktuell?

Hacker sind kreativ und anpassungsfähig, und sie versuchen auch die Situation der Pandemie für sich auszunutzen. So hat man einen Anstieg um ca. ein Drittel von Phishing und Spoofing-Attacken festgestellt. Dieses Niveau hält an. Die Sicherheitsmechanismen in einer Firma konzentrieren sich oftmals auf komplexe und fortgeschrittene Angriffstechniken. Doch in diesem Fall hat sich das Angriffsgeschehen auf den außerbetrieblichen Alltag verlagert. Dort geht das größere Risiko davon aus, dass Menschen dazu verlockt werden, unbekannte Programme auszuführen oder schadhafte Dokumente zu öffnen. Die Angriffstechniken sind alle nicht neu, werden aber auf Corona angepasst. Kommt es zu Attacken und Schäden im Homeoffice, ist das Unternehmen verantwortlich.

Auf diesem Gebiet ist BDO relativ neu. Bereits zwei Jahre nach Gründung der Tochter BDO Cyber Security im Sommer 2018 kann die Gesellschaft erste größere Erfolge vorweisen. Wie ist Ihre Strategie im Vergleich zu anderen?

Neu ist für BDO die Beschäftigung mit Cyber Security in Deutschland. Allerdings hat BDO heute schon ein weltweites Netzwerk in etwa 20 Ländern mit Cyber Security-Bereichen. Das ist ein großes Potenzial an Erfahrungen, Technologie und Mitarbeitern, mit dem wir uns in Deutschland natürlich vernetzen und und es uns dadurch zunutze machen. Hinzu kommt ein großes Netzwerk an Business-Partnern. Das versetzt uns in die Lage, Cyber Security ganzheitlich als Beratung und Dienstleitung anzubieten, bei aller thematischen Breite. Und ich glaube, dass hier ein entscheidender Unterschied zu vergleichbaren Beratungshäusern liegt.

Ihr BDO-Partner Ophir Zilbiger aus Israel sprach in seinem Vortrag über internationale Kontrollsysteme. Welches Know-how steckt dahinter und was planen Sie konkret?

In Israel betreibt BDO ein 24/7 Security Operation Center (SOC), dessen Leiter Zilbiger ist. Dort werden mit selbst entwickelter Technologie, basierend auf Cloud-Diensten und -Tools, eine große Anzahl internationaler Kunden aller Größenordnungen betreut. „Message Detection and Response“ ist im Klartext eine Echtzeitüberwachung der Kunden-Netzwerke bezüglich Auffälligkeiten mit einer lernfähigen Technologie. Dies ist eine ideale Ergänzung zu den üblichen Endpunkt-Technologien mit erheblich ausgeweiteten Möglichkeiten.

Sie bauen gerade auch hierzulande ein SOC für mittelständische Unternehmen auf. Wie ist der aktuelle Stand und was steckt konkret dahinter?

Angesichts der rasanten Entwicklung der Cyber-Technologien stellen wir uns die Frage, wie sich KMUs in einigen Jahren Cyber Security-Schutz werden leisten können. Dies wird immer mehr zum Spezialisten-Geschäft. Diese Firmen werden nicht mehr in der Lage sein, selbst das benötigte Know-how vorzuhalten. Deshalb bauen wir ein Service-Center, um entsprechende ready-to-run Services anzubieten. Dabei greifen wir auf bereits bei BDO existierende Technologien zurück – siehe Israel – entwickeln aber auch eigene Services wie z. B. sichere Schnittstellen. Wichtig für uns ist: Der Service und die Kundenbetreuung kommen aus Deutschland und unterliegen deutschen Sicherheitsstandards.

Professionelle Krisenbewältigung in acht Schritten

FACHWISSEN AUS VIELEN BEREICHEN NÖTIG — Vielen Zuhörern dürften im Vortrag von Cyber-Experte **Bodo Meseke** die Worte „Eine Krise ist ein Wendepunkt – zum Guten oder Schlechten" im Gedächtnis geblieben sein. Mit seinem Vortrag „Incident Response: Der Umgang mit der Krise – digital und analog" hatte Meseke denn auch des Pudels Kern getroffen. Meseke ist bei der Wirtschaftsprüfungsgesellschaft **Ernst & Young** (EY) im Bereich Forensic & Integrity Services tätig und beschäftigt sich dort mit der Bekämpfung von Wirtschaftskriminalität – das bereits seit 27 Jahren. Dazu gehört seit langem auch die Auswertung digitaler Daten. Ziel seines Vortrags war es weniger, den technischen Aspekt zu durchleuchten, sondern vielmehr, die Verantwortlichen in den Unternehmen grundsätzlich zum Nachdenken zu bringen, was es denn bedeute, eine (Cyber-) Krise zu managen. Die Ausgangsfrage seines Vortrags an die Teilnehmer war, ob sie sich die Zeit genommen hätten, sich auf eine Krise vorzubereiten oder ob sie eher überrumpelt wurden. Eine potenzielle Ausgangssituation ist etwa, wenn ein Unternehmen auf Anzeichen einer Verletzung des Schutzes personenbezogener Daten aufmerksam gemacht wird. Spätestens dann müssen die Alarmglocken schrillen. „Man tut jedenfalls gut daran, gut vorbereitet zu sein", lautet Mesekes Botschaft.

Bodo Meseke, Ernst & Young

Oberfläche für Cyberangriffe wird größer

Zur Bewältigung von Krisen gibt es viele Methoden. EY spricht dabei von der „Crisis Watch". Sie bietet Lösungsansätze zur Bewältigung von Vorfällen und zum Krisenmanagement. Die Uhr fängt an zu ticken, sobald der Vorfall bekannt und das Risiko vorhanden ist. Ab diesem Zeitpunkt startet eine Art Bergmarsch, so Mesekes bildhafte Beschreibung des beginnenden Interventionsprozesses, der über mehrere Stufen bis hin zum Gipfel verläuft. Da sich die Oberfläche für Cyberangriffe immer weiter vergrößert, erfordert eine effektive Reaktion auf einen Vorfall Know-how und Fachwissen aus vielen verschiedenen Bereichen. Geschulte Teams innerhalb des Unternehmens sind dabei stets die bevorzugte Lösung. Cyber-Experte Meseke weiß aber auch, dass viele Unternehmen nicht über spezielle Teams verfügen. Es sei daher unwahrscheinlich, eine geordnete Reaktion auf einen Vorfall innerhalb von 72 Stunden umzusetzen, wenn ein Unternehmen – intern oder in Zusammenarbeit mit externer Hilfe – nicht gut vorbereitet ist. Innerhalb dieser Zeit sollte im Rahmen der Kommunikationsstrategie (PR), die eine Stufe des Interventionsprozesses ist, die Benachrichtigung der Aufsichtsbehörde erfolgen, nachdem der Datenverwalter auf eine Verletzung des Schutzes personenbezogener Daten aufmerksam wurde.

Die Schritte davor sind zunächst die Validierung (1) bzw. die Suche nach dem Auslöser des Vorfalls. Es folgen die Bewertung erster Schäden und anderer Risiken (2) sowie die Bildung eines Kommando-Teams, das die Führung und Kontrolle bei der Krisenbewältigung in die Hand nimmt (3). Im nächsten Schritt heißt es, sich den Herausforderungen im Hinblick auf Schäden und Risiken zu stellen (4). Danach die schon erwähnte Krisen-Kommunikation (5). Ab jetzt heißt es, vorauszuschauen und so schnell wie möglich zum normalen Geschäftsablauf (6) zurückzukehren. Den Abschluss des „langen Bergmarschs" zur Bewältigung der Krise bilden Evaluation (7) sowie Reflexion (8). Die Überprüfung der gesamten Reaktionskette auf einen Vorfall sollte schließlich zu angemessenen Lerneffekten und Verbesserungen führen. ■

Assekuranz setzt auf forensische Dienstleistungen

KOOPERATION MIT SERVICE-PARTNERN — Mit einem etwas provokanten Titel „Cyber-Crime – Wegducken gilt nicht" hat **Carsten Wiesenthal** die bei der **Allianz** tatsächlich gemachten Schadenserfahrungen den Konferenz-Teilnehmern nähergebracht. Deutschlands größter Versicherer verfolgt auf diesem Gebiet einen holistischen Cyber-Lösungsansatz, der auf einer Betreuung der Kunden im gesamten Cyber-Risikomanagement-Prozess basiert. Neben einem ganzheitlichen Risiko Assessment, bei dem Unternehmen schon vor dem Vertragsabschluss ihr Cyber-Risiko besser verstehen lernen, sowie einem bedarfsgerechten Deckungskonzept und Schulungsmaßnahmen, glaubt Experte Wiesenthal, der Rechtsanwalt ist und bei der Allianz den Bereich MidCorp leitet, vor allem an die Zusammenarbeit mit ausgewählten Service-Partnern (z. B. **Computacenter, Metafinanz**), wie es auch andere Versicherer tun. Hier stehen forensische Dienstleistungen im Vordergrund, um die Schadensauswirkung gering zu halten und mit einer geeigneten Krisenkommunikation die Situation zu meistern. Einen hundertprozentigen Cyber-Schutz gibt es nicht. Darin waren sich die Referenten auf dem 2. PLATOW UnternehmerFORUM einig. Für das Restrisiko stehen im Schadensfall mittlerweile über 40 Versicherungsgesellschaften mit Deckungsschutz zur Verfügung. ■

Carsten Wiesenthal, Allianz