logistikroundtable

WWW.VERKEHR.CO.AT

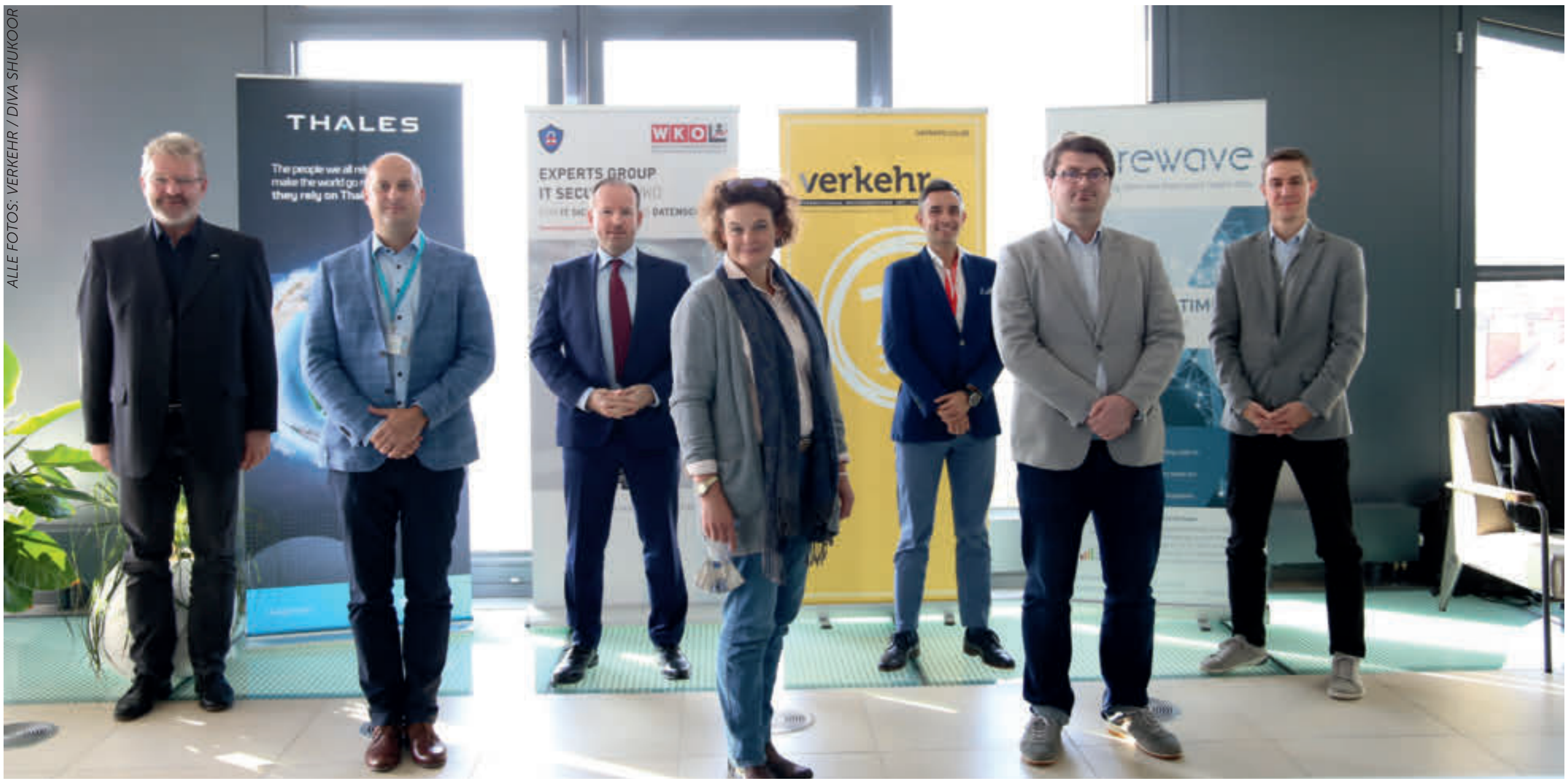
EIN SPECIAL DER INTERNATIONALEN WOCHENZEITUNG VERKEHR

Nr. 44-45
76. Jahrgang
06.11.2020

Risikoprävention – wie können sich Unternehmen schützen?

ROUND TABLE: Die Logistik wird immer digitaler und vernetzter, was zunehmend die Gefahr von Angriffen aus dem Cyberspace für Unternehmen erhöht. *Verkehr* wollte deshalb von fünf Experten wissen, wie man Gefahren (vorausschauend) erkennen und abwehren kann.

ALLE FOTOS: VERKEHR / DIVA SHUKOOR



(v.l.n.r.) Thomas Glade (Leiter des Universitätslehrgangs Risikoprävention und Katastrophenmanagement an der Uni Wien), Christian Linhart (Sales Director Austria & CEE, DIS/CPL BU Data Protection Thale Austria), Harald Wenisch (Sprecher der ExpertsGroup IT Security WKÖ), Claudia Hefelle (Redakteurin der Internationalen Wochenzeitung Verkehr), Árpád Geréd (IT-Experte und Anwalt bei MGLP Rechtsanwälte), Muhamed Beganović (Chefredakteur der Internationalen Wochenzeitung Verkehr) und Harald Nitschinger (Geschäftsführer Prewave)

VON MUHAMED BEGANOVIĆ UND CLAUDIA HEFELLE

Verkehr: In der Logistik nimmt das Thema Digitalisierung einen immer höheren Stellenwert ein. Jede neue Chance bringt jedoch neue Risiken. Hat das Bedrohungspotenzial in den vergangenen Jahren zugenommen?

Harald Wenisch: Die Risiken haben deutlich zugenommen, und die Spitze ist bei Weitem noch nicht in Sicht. Die Digitalisierung hat den Zenith noch lange nicht erreicht. Große Unternehmen haben hier schon vieles professionell umgesetzt, aber kleine und mittlere Unternehmen (KMU) stehen teilweise erst am Anfang. Außerdem kommen bei KMU durch die Konvergenz verschiedener Arbeitsbereiche, etwa bei Banken, kritischer Infrastruktur oder Telekommunikation, immer neue Produkte und Mittel auf den Markt, womit die Risiken größer werden. Daher ist es wichtig, eine gute Infrastruktur und ein gutes Netzwerk aufzubauen, das im Bedarfsfall kompakte Lösungen bietet.

Christian Linhart: Wir sehen hier die Spitze des Eisbergs. Zum einen steigt das Datenwachstum rasant, zum anderen haben wir durch die Pandemie jetzt das Problem, dass sich Ressourcen verteilen müssen. Das heißt: Mitarbeiter, die früher im Betrieb für die IT-Security zuständig waren, arbeiten plötzlich von zu Hause aus. Es gilt, die Workload zu organisieren und zu kontrollieren. Und: Die „dunkle Seite der Macht" schläft nicht, sondern sie hat einfache und effektive Methoden herausgefunden, wie mit Unternehmen, die nicht entsprechend vorgesorgt haben, Geld zu machen ist, indem sie das Chaos ausnützen. Wir werden uns auf neue Methoden und Szenarien der Bedrohung sowie gezielte Attacken einstellen müssen.

Wohin gehen hierbei die Trends?

Linhart: Aktuell ist es Erpressung, früher war beispielsweise Datenklau ganz oben auf der Liste. Damit lässt sich relativ einfach Geld verdienen, da man Unternehmensdaten verkaufen oder das betroffene Unternehmen selbst mit Ransomware stilllegen kann.

AUSGANGSSITUATION

Während die Bundesregierung bereits über den zweiten Lockdown in Österreich Beratungen abhielt, analysierte eine Gruppe von Experten am Sitz der Firma Thales in Wien Risiken und Auswirkungen derartiger Ausnahmesituationen. Anlass war ein Roundtable-Gespräch der Internationalen Wochenzeitung *Verkehr* zum Thema „Risikoprävention"; moderiert wurde die Diskussion von Muhamed Beganović, Chefredakteur der Internationalen Wochenzeitung *Verkehr*. Christian Linhart (Sales Director, Austria & CEE, DIS/CPL BU Data Protection Thales Austria), Thomas Glade (Leiter des Universitätslehrgangs Risikoprävention und Katastrophenmanagement Uni Wien), Árpád Geréd (IT-Experte und Anwalt bei MGLP Rechtsanwälte), Harald Wenisch (Sprecher der ExpertsGroup IT Security WKÖ) sowie Harald Nitschinger (Geschäftsführer von Prewave, einem Start-up, das mittels Analysetools in Social-Media-Kanälen Gefahren für Lieferketten und Produktion frühzeitig ermittelt) brachten ihre praxisaffinen Erfahrungen und Expertisen zum Thema ein. Zunächst widmeten sich die Experten speziell den neuen Bedrohungen aufgrund von Digitalisierung und Globalisierung. Mit der Corona-bedingten Umstellung auf Homeoffice-Arbeitsplätze wurden viele zuvor wenig beachtete Bedrohungen plötzlich virulent. Aber nicht nur virtuelle Gefahren lauern, auch Naturkatastrophen oder Blackouts können zum Risiko werden. Präventionsmaßnahmen sowie Datenschutz und Compliance fanden ebenso Eingang in die spätere Diskussion wie der Schutz von kritischer Infrastruktur und sensiblen Lieferketten.

FORTSETZUNG AUF SEITE 2

FORTSETZUNG VON SEITE 1

Harald Nitschinger: Sowohl die Digitalisierung als auch die Globalisierung bringen neue Bedrohungspotenziale mit sich. Wir arbeiten vor allem mit Unternehmen aus der Automobilindustrie und deren Zulieferern sowie mit Elektronikproduzenten zusammen. Durch die steigende Komplexität der Lieferketten in einer globalisierten Welt ist die Angriffsfläche für externe Risiken wie einen Hafenstreik, Industrieunfall, eine Naturkatastrophe oder eben eine Pandemie extrem gestiegen.

Árpád Geréd: Als Anwalt, der auf IT und Security spezialisiert ist, sehe ich vor allem meine Aufgabe darin, dass das, was es an Allgemeinpflichten und speziellen Vorschriften gibt, in Unternehmen richtig umgesetzt wird. Gerade für KMU fehlen hier aber entsprechende Richtlinien, was mindestens verlangt wird. Die Zwangsdigitalisierung, die mit der Pandemie gekommen ist, und Homeoffice, beflügeln sowohl die Unsicherheit als auch das Risikopotenzial. Nicht nur in der Transport- und Logistikbranche können größere Player einfacher diese Herausforderungen abfedern, sondern zusätzlich auch Hilfestellung leisten, denn innerhalb der Lieferketten gibt es KMU, die dabei auf die Unterstützung der Größeren – etwa bei der Erstellung von Mindeststandards – angewiesen sind. Hier wären auch infrastrukturelle Vorkehrungen denkbar, um in technischen Verbindungen gezielt Flaschenhälse zu schaffen, die gut kontrollierbar sind. Sollte also ein kleiner Zulieferer Opfer eines – heute schon maßgeschneiderten – Ransomware-Angriffs sein, wäre der Konzern nicht unmittelbar betroffen.

Ein Aspekt, der hinsichtlich der Verantwortlichkeit und Haftung auch an Bedeutung gewinnt, ist zweifellos die Mitarbeiter-Schulung. Homeoffice bietet bedeutende Angriffsflächen und E-Mails werden gezielt gefälscht. Mitarbeiter-Schulung ist daher ein Grundpfeiler jeder IT-Security, besonders wenn alleine und von zu Hause aus gearbeitet wird, um sich selbst sowie die gesamte Supply Chain und Kunden abzusichern.

Also jeder ist nur so stark wie das schwächste Glied in der Kette?

Thomas Glade: Unser Studienlehrgang wurde für solche Szenarien ins Leben gerufen. Im Kontext der Digitalisierung fällt auf, dass diese genau das beinhaltet, was wir wissenschaftlich als Vulnerabilitäts-Paradoxon bezeichnen. Das heißt: Man wird immer besser, weil Informationen immer schneller, global und besser zugänglich sind; auf der anderen Seite macht man sich zunehmend abhängiger, und wenn der Zugang zu den Informationen wegfällt, ist die Katastrophe noch größer. Der zweite Punkt betrifft die ansteigende Unsicherheit, wenn Kaskadeneffekte auftreten. Es ist eine große Herausforderung zu lernen, mit Dingen umzugehen, ohne sich vorher darauf einstellen zu können, um damit das Kippen des Systems zu verhindern. Hierbei ist die Digitalisierung ein großer Schwachpunkt, aber gleichzeitig eine große Stärke.

Nitschinger: Kaskadeneffekte können in ganz verschiedenen Szenarien auftreten. Wir haben 14 Tage im Voraus Hafenstreiks erkannt, weil gewisse Kaskaden durch Drohungen, Ankündigungen etc. ausgewertet werden konnten. Auch bei der Corona-Pandemie haben wir 10 bis 14 Tage vorher vor dem Shutdown bei Lieferanten gewarnt, weil dies in den sozialen Medien über Infektionsfälle, Streikdrohungen etc. ersichtlich war, ehe die regionalen und überregionalen Reaktionen tatsächlich erfolgten. Diese Kaskaden identifizieren wir in sozialen Medien und schicken entsprechende Warnungen. In puncto Cyberrisiko sind diese Dinge schwieriger, weil sie im Verborgenen passieren. Unsere Technologie funktioniert gut im öffentlichen Bereich, aber im Cyberspace brauche ich jedoch andere Instrumente.

Glade: Die Identifikation ist eine Sache – aber der nächste Schritt heißt: Was mache ich damit? Und das ist eine Sache der Ausbildung, um präventiv auf verschiedene Schritte in einer Kaskade reagieren zu können und Handlungsoptionen zu sehen.

> „DURCH DIE STEIGENDE KOMPLEXITÄT DER LIEFERKETTEN IN EINER GLOBALISIERTEN WELT IST DIE ANGRIFFSFLÄCHE FÜR EXTERNE RISIKEN EXTREM GESTIEGEN." – HARALD NITSCHINGER

Homeoffice ist seit Corona verstärkt im Fokus. VPN-Netzwerke sollten Standard sein, doch besonders bei Videokonferenzen hat sich gezeigt, wie anfällig dieses Instrument dafür ist, angezapft zu werden. Durch social engineering werden E-Mails quasi maßgeschneidert. Wie kann sich ein Unternehmen davor schützen?

Linhart: Mitarbeiterschulungen sind hier das A und O. Es gibt verschiedenste Mitarbeiter- und Awareness-Schulungen – und gerade bei einem Unternehmen wie Thales gehört das zum täglichen Brot. Wir alle werden regelmäßig gebenchmarkt und high-sophisticated Angriffen unterzogen; das ist bei uns ein Routineablauf. Ich sehe jetzt aber zum Glück schon bei vielen anderen Unternehmen mehr Investitionen in die Mitarbeiter, um sie entsprechend zu schulen. Technische Hilfsmittel, die State of the Art sein sollten, erlebten, gerade zu Beginn der Pandemie einen Run, weil viele Unternehmen noch ziemlich blank waren, etwa bei klassischen Multifaktor-Autorisierungs- und Accessmanagement-Lösungen, wie sie Thales anbietet. Username- und Passwort-Autorisierungen reichen für Homeoffice-Arbeitsplätze definitiv nicht aus. Das ist der erste Schritt, denn ein Angreifer geht den einfachsten verfügbaren Weg: Er hackt sich nicht ins Unternehmen, sondern loggt sich einfach ein! Da gibt es in vielen Firmen Nachholbedarf!

Wenisch: Ich glaube, unsere Runde ist sich einig, dass mit der Globalisierung und Digitalisierung neue Lösungen für die Wirtschaft und für Unternehmen weiterentwickelt werden müssen. Dabei braucht es drei Schwerpunkte: Awareness, also die Kenntnis der Unternehmer, wo Risiken lauern, Know-how in den unterschiedlichsten Bereichen top-down und natürlich das Thema Tools, das für Europa noch stark fehlt, gerade wenn es um Supply Chains geht. Wir sind hier nach wie vor mit den Basics beschäftigt!

Geréd: Die Geschäftsführung

muss verstehen, dass Geld, welches hier investiert wird, nicht die Anschaffung eines neuen technischen Spielzeugs darstellt, sondern wesentliche Auswirkungen auf den Geschäftsbetrieb und die rechtliche Verantwortung sowie auf die Unternehmenszukunft hat. Und es ist wichtig, das rechtzeitig zu kommunizieren, damit am Ende des Tages nicht Zeit oder die Mittel fehlen, um eine Lösung ordentlich umzusetzen.

Wenisch: Das stimmt – IT-Security wird bis heute noch als Kostenfaktor gesehen. Leider fehlen hier aber auch entsprechende Produkte, die Substanzielles verbessern.

Glade: Wir arbeiten immer stärker zusammen und sind im Rahmen der Globalisierung sehr gut organisiert. Wir haben mit zunehmend komplexeren Situationen zu tun, in denen immer mehr verschiedene Parteien, die ein unterschiedliches semantisches Verständnis haben, involviert sind. Und genau das ist in unserem Lehrgang ein wichtiger Punkt: zu vermitteln, dass es ganz unterschiedliche Auffassungen und Sichtweisen gibt, die man begreifen muss, um im Entscheidungsfall gut miteinander kommunizieren zu können – im Katastrophenfall sogar unter enormem Zeitdruck. Viele Mitarbeiter auf der Führungsebene sind dafür aber gar nicht mehr ausgebildet, weil sie zu spezialisiert sind und verlernt haben, holistisch zu denken und das Wissen von anderen positiv zu nutzen.

Nitschinger: Was sich hier als hilfreich erweist, sind Standards. In der Automobilindustrie ist es zum Beispiel die Macht des Herstellers, der in seine Lieferkette einen gewissen Zwang hineinbringt, um verschiedene Normen und Standards zu erfüllen. Das betrifft selbst uns als kleines IT-Start-up; aber es macht Sinn.

Wenisch: Sind wir uns aller Standards und Vorgaben bewusst, die auf den Unternehmer wirken? Ich selbst tue mir als Sachverständiger manches Mal schwer, den Überblick über alle wechselnden Regelungen zu behalten. Ich sehe das beim Thema CDISE: IT ist ein offenes Gewerbe, deshalb hat der Fachverband das Qualitätssigel Certified Data and IT-Security-Expert geschaffen, das auf Basis einer ISO-17024-Norm persönlich die Qualifizierung feststellt. Mittlerweile haben wir über 500 ausgebildete Experten am österreichischen Markt. Wir sind als kleines Land durchaus Vorreiter, denn wir haben in Österreich nicht nur einen Expertenstandard im Sicherheitsumfeld geschaffen, sondern auch eine Cyber-Security-Hotline, die in Europa einzigartig ist. Gerade KMU haben oft das Problem, dass sie im Bedarfsfall nicht wissen, an wen sie sich im cybertechnischen Notfall wenden sollen. Die Security-Experts-Group ist eine Anlaufstelle für Unternehmer und Experten, die diese Plattform zusammenbringt. Diese Hilfestellung ist in Österreich kostenlos und sehr innovativ.

Stichwort Acces-Management. Im Logistikbereich ist in den vergangenen Jahren das Angebot an Buchungsplattformen gestiegen, auf denen ich mich als Firma direkt in einem anderen Unternehmen einlogge und Berechtigungen freigebe etc., was selbstverständlich ein Risiko bedeutet. Wie können sich Unternehmen hier effektiv schützen?

Linhart: Thales ist eines der wenigen globalen und vor allem europäischen Cyber-Security-Unternehmen, die hier eine starke Expertise mitbringen. Einer dieser Standards ist die Verschlüsselung von kritischen Unternehmensdaten, um diese im Falle einer Databreach geschützt zu haben. Diese Verschlüsselung ist quasi der Sicherheitsgurt für Daten, und wir bieten verschiedene Lösungen on premise oder in der Cloud an. Datensicherheit ist mittlerweile so komplex geworden, dass Unternehmen oft keinen Überblick mehr haben, wo ihre Daten tatsächlich gespeichert sind. Wir haben dafür spezielle Lösungen, die sicherheitsrelevante Daten finden und klassifizieren können bzw. diese schützen. Freilich muss sichergestellt sein, wer genau auf die Daten zugreifen kann – und dieser Zugriff soll nachweisbar sein.

Wenisch: Compliance bekommt in den nächsten Jahren sicher noch mehr Drive, speziell für den KMU-Bereich. Man darf gerade in Österreich nicht vergessen, dass viele der Unternehmen Teil wichtiger Lieferketten sind. Umso relevanter wird dabei das Thema Strafen, die wir den Unternehmern nach Möglichkeit ersparen wollen, indem wir entsprechende Prävention anbieten.

Linhart: Die Technologien existieren, aber sie werden noch zu wenig genutzt. Einzug finden diese Lösungen leider oft erst dann, wenn ein Unternehmen selbst betroffen ist.

„DIE ‚DUNKLE SEITE DER MACHT' HAT EINFACHE METHODEN HERAUSGEFUNDEN, WIE MIT UNTERNEHMEN, DIE NICHT VORGESORGT HABEN, GELD ZU MACHEN IST." – CHRISTIAN LINHART

Wenisch: Ich glaube nicht, dass die Technologien bereits in der nötigen Nutzerfreundlichkeit existieren, denn für normale mittelständische Unternehmen sind diese Tools oft viel zu kompliziert in der Verwendung. Die Usability muss verbessert werden und die Konzepte müssen einfacher zu verstehen sein, damit sie in die Praxis umzusetzen sind, nur dann funktioniert etwas. Das fehlt uns bis heute: Tools in der entsprechenden Konfiguration, weniger abstrakte Normen und mehr Awareness.

Geréd: Hinsichtlich der Normen dürfen wir uns in den nächsten Jahren wohl nicht allzu viel erwarten. Hilfestellungen passieren in Form von neuen Ideen, die am Markt auftauchen, oder anhand von ganz konkreten Beispielen wie in der NIS-Richtlinie oder auch mittels der DSGVO. In Mitarbeiter-Schulungen, Veranstaltungen etc. kann man diese Beispiele des Gesetzgebers aufgreifen, anhand derer man eigene nutzbare Lösungen präsentiert – auch in der eigenen Supply Chain, wo Standards eigenständig gesetzt werden, weil der Gesetzgeber natürlich langsamer ist. Über diese Absicherungsketten wird es zukünftig wahrscheinlich besser funktionieren, Compliance umzusetzen und die Firma selbst und ihre Supply Chain zu schützen, ohne die Menschen mit abstrakten Anforderungen zu überfordern.

Wenisch: Wir leben in einer globalisierten Welt, aber aufgrund der unterschiedlichen Rechtssysteme muss immer die richtige Interpretation gesucht werden. Das Beispiel DSGVO gefällt mir besonders gut, denn mit allen Erwägungsgründen und Ausnahmen wird das Thema sehr komplex. Insofern ist es besonders wichtig, die Experten auf dem Laufenden zu halten, um eine verlässliche Informationsquelle zu bieten.

Nitschinger: Es ist essenziell, dass Compliance und Standards in der Lieferkette wirken, um es so auch in die Fläche zu bringen. Die Covid-Krise hat offenbart, dass bei vielen Kunden diese Strukturen noch fehlen – und damit meine ich nicht nur den Bereich IT-Security: Wir haben festgestellt, dass absolut reaktiv vorgegangen wird, wenn die Katastrophe oder Krise da ist.

FORTSETZUNG AUF SEITE 4

SHUTTERSTOCK / WUTZKOHPHOTO

FORTSETZUNG VON SEITE 3

Selbst global agierende Milliardenkonzerne verfügen über keine strukturierten und vordefinierten Prozesse, um diese Kommunikation abzuwickeln. Und dabei geht es beispielsweise um die Abfrage tausender Lieferanten! Es fehlt oft an grundlegenden Strukturen, um mit einer Krise umgehen zu können. Und diese Strukturen müssen vorher geschaffen werden.

Wenisch: Ich muss ihnen widersprechen: Ich glaube, es gibt diese Strukturen in den großen Unternehmen, aber sie werden zu wenig geübt. Bei Cyber-Planspielen, gemeinsam mit der Wirtschaftskammer und dem Innenministerium, konnten Unternehmen einen Tag lang eine definierte Cyberkrise sehr dynamisch durchspielen. Das Interessante: Szenarien und entsprechende Prozesse waren zwar ausformuliert, aber wurden in der Praxis nie über die einzelnen Abteilungen hinaus geübt. Zwischen Theorie und Praxis muss Raum zugelassen werden, wo solche Szenarien stattfinden können. In Bezug auf Resilienz sind Planspiele etwa eine wichtige Information, die die Lieferketten in schwierigen Situationen am Leben erhält und Mehrwert für den Regelbetrieb schafft, auch bei Investitionen.

Nitschinger: Dem kann ich zu 100 Prozent beipflichten: Herangehensmuster, wie sie im militärischen Umfeld geübt werden, müssen auch im Supply Chain Management ankommen. Die Pläne müssen gelebt werden können, und genau das hat die Krise offenbart: Es wurden gnadenlos die Schwächen aufgedeckt – auch dort, wo Strukturen vielleicht

„IT-SECURITY WIRD BIS HEUTE ALS KOSTENFAKTOR GESEHEN. LEIDER FEHLEN HIER ABER AUCH ENTSPRECHENDE PRODUKTE, DIE SUBSTANZIELLES VERÄNDERN.“ – HARALD WENISCH

„Datensicherheit ist mittlerweile so komplex geworden, dass Unternehmen oft keinen Überblick mehr haben, wo ihre Daten tatsächlich gespeichert sind“, gibt Christian Linhart zu bedenken

theoretisch vorhanden, aber nicht praktisch geübt worden sind.

Gefahren für die Supply Chain lauern nicht nur in der virtuellen Welt. Erdbeben oder Überschwemmungen sorgen immer wieder für Unterbrechungen in der Lieferkette. Wo sehen Sie die größten Bedrohungsszenarien für die nächsten Jahre?

Glade: Denke das Undenkbare! Selbst eine verhältnismäßig kleine Störung kann alles zusammenbrechen lassen. Unternehmen muss der wirtschaftliche Mehrwert von Präventivmaßnahmen vor Augen geführt werden, beispielsweise in Form von Planspielen. Gerade Logistikfirmen sollten ein Augenmerk auf ihre Knackpunkte und sensiblen Stellen richten. Im Ereignisfall müssen oft wichtige Entscheidungen, die global wirken, sehr rasch getroffen werden. Und genau das erfordert Übung: unter großer Unsicherheit rasch zu entscheiden und verschiedene Optionen zu erkennen. Für mich ist die Prävention wesentlich, egal für welches Ereignis als Auslöser. Was passiert, wenn jetzt kein Strom mehr da ist oder es ein Erdbeben gibt? Gerade jene Dinge, die am unwahrscheinlichsten sind, haben meist den größten Impact, wie die Pandemie aktuell zeigt; deshalb müssen wir uns mit ihnen auseinandersetzen. Bereits der Ausfall eines einzelnen Lieferanten kann gigantische Folgen haben. Gerade das Denken in komplexen Systemen soll durch unseren Studiengang vermittelt werden, denn im Katastrophenfall müssen ganz unterschiedliche Systeme zusammenarbeiten können.

„Der Faktor Mensch wird bei aller Globalisierung, Technologie etc. immer wichtiger, weil die Kommunikation selbst immer wichtiger wird“, betont Harald Wenisch

Haben Sie nach fünf Jahren Lehrgang das Gefühl, dass die Awareness für dieses Thema zugenommen hat?

Glade: Ja, vor allem zahlen zunehmend Unternehmen die Studiengebühren, was zeigt, dass realisiert wird, dass diese übergeordnete Ausbildung einen Mehrwert generiert. Gerade von den ersten Absolventen hören wir oft, dass Firmen zusätzliche Kosten scheuen und den Wert – zumindest vor Corona – noch nicht erkennen konnten. Ich glaube, dass die Covid-Krise gesellschaftlich ein Umdenken herbeigeführt hat, dass es für Firmen eben rentabel ist, über entsprechend ausgebildete Leute zu verfügen.

Prewave beschäftigt sich speziell mit Themen wie Streiks oder Brexit. Was bedeutet beispielsweise ein harter Brexit mit allen Begleiterscheinungen für die Lieferketten und wie kann man hier proaktiv agieren?

Nitschinger: Dieses Ereignis kommt nicht wirklich überraschend. Die Globalisierung macht das Unwahrscheinliche wahrscheinlicher und ein Hafenstreik oder ein Waldbrand in Indonesien oder ein Tsunami in Asien hatte früher wenig Auswirkungen auf die österreichische Wirtschaft. Dem ist heute nicht mehr so. Wir haben unseren Wohlstand auf globale Risiken exponiert, der gerade durch die Effizienz auch auf wackeligeren Beinen steht. Unser Beitrag ist in erster Linie einmal die Information, was der erste Step in einem verlässlichen Krisenmanagement ist. Die nächsten Ebenen sind Bewertung und Kommunikation mit Lieferanten, wo wir anhand von Corona auch die Notwendigkeit von neuen Kommunikationskanälen gesehen haben. Unsere Kunden schicken nun nicht mehr Listen, sondern eine ganz klare Anfrage an Lieferanten, die wiederum mit Grün, Gelb, Rot antworten. Damit geht man dann in die Lösung. Durch Covid wurde das Bewusstsein für das Risikomanagement gestärkt sowie die Reduktion der niedrigen Lagerstände und der Globalisierung hinterfragt.

Glade: Mein Credo war immer ein faktenbasiertes Wissen als Basis für Handlungen. Nun sehe ich in den letzten zwei Jahren aber zunehmend Entwicklungen, bei denen faktenbasiertes Wissen keine Rolle mehr spielt, indem Dinge einfach verneint werden. Hier wurden mit sozialen Medien neue Kanäle und Möglichkeiten geschaffen, die früher noch nicht existierten. Impulse von relativ kleinen Gruppen, die vollkommen irrational sind, können dennoch ein ganzes System erschüttern. Das müssen auch große Firmen lernen: den Umgang mit falschen Behauptungen, denn Fakenews können genauso auf Versorgungsflüsse Einfluss nehmen. Diese Beispiele müssen wir ebenfalls noch stärker integrieren. Für den Verkehr und die Logistik ist es extrem wichtig, diese Szenarien immer mitzudenken, denn wenn die Situation aufkommt, muss klar sein, wer wie reagiert, und zwar sehr rasch.

Wenisch: Das passt gut zu meiner Wahrnehmung, dass der Faktor Mensch bei aller Globalisierung, Technologie etc. immer wichtiger wird, weil die Kommunikation selbst immer wichtiger wird.

Geréd: Es verändern sich die Faktoren im Hintergrund: Business Intelligence sollte ich heute auch dazu nutzen, meine Supply Chain abzufragen. Ich sollte aus der Krise Rückschlüsse für meine Zukunft ziehen – aber die Ressourcen, die mittlerweile sowieso mehrheitlich überspannt sind, bleiben dennoch gleich. Uns muss im rechtlichen Kontext bewusst sein, dass wir trotz allen

Wunschdenkens rational mit dem arbeiten müssen, was wir haben, natürlich vor dem Hintergrund der Compliance und in Hinblick auf mögliche zukünftige Gewichtung der einzelnen Faktoren. Wir als Unternehmen müssen also entscheiden, ob in die Supply Chain investiert werden soll, um Verstößen vorzubeugen, oder in IT-Security zum besseren Schutz oder ob es sinnvoll ist, nicht überhaupt eine ganz neue Kommunikationsebene zu erzeugen. Unternehmen müssen hier ihre eigenen Rückschlüsse ziehen dürfen, denn die Antworten auf viele Fragen werden wir erst in mehreren Jahren erhalten.

Nitschinger: Das ist die Kunst, Information zu aggregieren und Desinformation zu verhindern. Kunden wollen auf einen Blick sehen, welchen Status etwa ein Lieferant hat.

Geréd: Und genau das muss irgendwann auch in KMU und der gesamten Supply Chain ankommen.

Wir haben die Themen Lizenzierung, Forschung und Analytik besprochen; aber das alles wäre ohne Big Data nicht in dieser Form möglich. Hier kommt nun das Thema Datenschutz ins Spiel ...

Geréd: Datenschutz ist ein Reizwort für viele Unternehmen, für andere ist es das neue Gold.

Die Logistik hat im oberen Drittel der Anbieter den Vorteil, dass sie sich technisch und organisatorisch sowieso schon so stark gegen andere Risiken schützen muss, dass Datenschutz mit herkömmlichen Mitarbeiter- und Kundendaten nicht mehr wesentlich ins Gewicht fällt. Schwieriger wird es in jenen Branchen, wo man unvorbereitet war, oder beispielsweise bei KMU, die plötzlich von Geschäftspartnern vordefinierte Standards, die am besten international gelten sollten, innerhalb der Supply Chain erfüllen müssen. Mit der DSGVO ist die Technologie auf rechtliches Gebiet eingedrungen; davor war es ein formelles Thema. Mittlerweile braucht es eine technische Lösung, um compliant zu sein. Gerade innerhalb der Lieferketten sind diese technischen und organisatorischen Maßnahmen, die ich ergreifen muss, um datenschutzrechtlich compliant zu sein, auch eine Absicherung des Geschäftsumfelds selbst. Sie sind eine zwingende Notwendigkeit, um den Betrieb aufrecht zu erhalten und zu verhindern, dass Daten verschwinden oder Einfluss auf die Supply Chain genommen werden kann.

Wie sammelt man Daten denn richtig bzw. wie sammelt man die richtigen Daten?

Linhart: Das Datenwachstum steigt, und ich muss sicherstellen können, dass dieses Material auch integer ist, weil es aus glaubwürdigen Quellen meiner Systeme kommt. Was passiert aber, wenn jemand nicht nur meine Daten abgreift, sondern diese auch manipuliert? Die nicht offensichtliche Verschiebung von einigen Kommastellen oder in Formeln könnte aufgrund der darauf basierenden Entscheidungen mein Unternehmen innerhalb weniger Jahre ruinieren. Daher müssen Daten möglichst manipulationssicher und am besten unter dem Gesichtspunkt der Gewaltentrennung gespeichert werden. Ich muss technologisch einen genau definierten Benutzerkreis festlegen, der mit diesen Daten agieren darf. Dabei helfen Tools wie Accessmanagement und Verschlüsselung.

Herr Nitschinger, Sie werten für Ihre Plattform Prewave Daten in 50 verschiedenen Sprachen und aus verschiedensten sozialen Medien und Nachrichtenplattformen aus. Zwischen Information und Desinformation liegen nur drei Buchstaben – wie filtert man Wahrheit und Lüge?

Nitschinger: Das ist eine der Kernfragen seit Anbeginn der Forschung, wie relevante und valide Informationen extrahiert werden können. Dazu gibt es mehrere Anknüpfungspunkte. Klassische Fakenews finden in den sozialen Medien noch auf einer sehr breiten Ebene mit eher schwammigen Themen statt. Unsere Technologie ist jedoch darauf ausgelegt, reale Ereignisse in der physischen Welt zu erkennen, womit wir uns auf einer sehr granularen Mikroebene befinden: ein Streik hier, ein Brand dort, die Infektion eines Mitarbeiters etc. Auch dabei kann natürlich manipuliert werden, aber sehr selten. Wir geben einen Risiko-Alert nie wegen einer einzelnen Quelle heraus, sondern immer aufgrund von gebündelten Informationen – sei es eines Shutdowns oder Streiks, wie es eben real passiert. Wir überprüfen aus dieser Gruppe von Quellen, wie diese strukturiert sind. Anhand unseres Tools erkennen wir damit das Risiko, welche Transportknotenpunkte oder Lieferanten potenziell betroffen sind, und schließlich können dann auch Betroffene darauf antworten und gegebenenfalls relativieren.

Wenisch: Ich glaube, dass wir beim Thema Daten noch viel zu sehr Schwarz-Weiß sehen. Ein relevantes Thema für die Logistik ist die Interpretation der Daten aus den Lieferketten. Das wird in naher Zukunft neue Berufsbilder kreieren: Leute, die mit Data Science viel stärker arbeiten. Und es ist wichtig, dass man das in der Ausbildung schon früh berücksichtigt. Die Fehlinterpretation und Manipulation von Daten wird ein Geschäftsfeld seitens der Kriminalität werden, was bis jetzt noch kein Thema ist: Wenn scheinbar alles funktioniert, aber trotzdem verändert wurde – das wird eine wirkliche Herausforderung.

„UNTERNEHMEN MUSS DER WIRTSCHAFTLICHE MEHRWERT VON PRÄVENTIVMASSNAHMEN VOR AUGEN GEFÜHRT WERDEN, BEISPIELSWEISE IN FORM VON PLANSPIELEN.“ – THOMAS GLADE

Welche Daten sammelt und interpretiert der universitäre Bereich für das Katastrophen- und Krisenmanagement?

Glade: Ich möchte grundsätzlich noch auf die Schwierigkeit von Entscheidungen eingehen, die auf einer breiten Basis von Fakten/Daten gefällt werden. Dabei müssen Schwellenwerte identifiziert werden, aufgrund derer üblicherweise Handlungen ausgelöst werden. Diese Daten sind jedoch nicht stationär, sondern die Quellen ändern sich kontinuierlich. Wie aussagekräftig sind meine alten Daten also noch für heute? Gleichzeitig brauchen wir diese Daten aber, um Szenarien zu berechnen und zukünftige Entwicklungen abzuschätzen. Wenn also Frühwarnsysteme in verschiedenen Kontexten etabliert sind wie Sensorik bei Naturereignissen oder Frühwarnsysteme im Entscheidungsprozess bei Firmen oder in der Logistik, befinden wir uns in dynamischen Systemen. Das heißt, dass solche Systeme kontinuierlich angepasst werden müssen. Und: Deren Dynamik wird immer höher, während wir mit unseren Entscheidungsprozessen permanent hinterherstolpern. Dafür kann ich leider keine Lösung anbieten. In der Ausbildung gehen wir aber immer mehr von fixen Konzepten ab und lehren stattdessen verschiedene Herangehensweisen und auch, dass vielleicht unsere heutigen Annahmen bald aufgrund neuer Daten oder auch neuer Konzepte obsolet sind, etwa durch neue Möglichkeiten wie Artificial Intelligence etc. Grundlegend bin ich aber der Meinung, dass Daten in jedem Fall Persönlichkeitsrechte darstellen.

„Es ist essenziell, dass Compliance und Standards in der Lieferkette wirken, um es so auch in die Fläche zu bringen. Die Covid-Krise hat offenbart, dass bei vielen Kunden diese Strukturen noch fehlen“, erläutert Harald Nitschinger

Nitschinger: Künstliche Intelligenz (KI) basiert ja in der Regel auf großen Datenmengen, statistisch modelliert, denn die Statistik deckt immer den Regelfall ab. Dinge wie Corona sind die Singularität, das ist das Gegenteil des Regelfalls – und deswegen werden sie in statistischen Modellen nicht repräsentiert. Die klassische Vorhersage für Lieferzeitpunkte wie bei Amazon oder Zalando kämpft damit, Unregelmäßigkeiten abzubilden. Und genau hier liegt die Grenze für klassische Big-Data-Ansätze, KI nur basierend auf statischen Modellen und historischen Daten zu betreiben. Deswegen braucht es Echtzeit-Daten, die neue dynamische Komponenten mithineinbringen. Hierhin bewegt sich das System.

Glade: Genau, denn: Wie repräsentativ ist der statistische Mittelwert? Ich empfehle meinen Studenten, sich für die Ausschläge zu interessieren. Das sind nicht immer Fehler, sondern oft Faktoren, die aufzeigen, dass es sich um ein viel komplexeres System handelt. Das ist auch für das Management ein wichtiger Zugang!

Wenisch: Wenn man jetzt an einen Leser aus der Logistikbranche denkt, dann sollte man bedenken, dass österreichische Unternehmen eine valide Datenquelle benötigen, mit der sie arbeiten. Manche Firmen haben schon zwei oder drei Mal ihre gesamten Datenbestände verloren. Da ist es wichtig, sich darauf verlassen zu können, wo und wie man diese Daten wiederbekommt, um auch das Thema Business Continuity hier anzusprechen.

„Mit der DSGVO ist die Technologie auf rechtliches Gebiet eingedrungen; davor war es ein formelles Thema. Mittlerweile braucht es eine technische Lösung, um compliant zu sein“, macht Árpád Geréd deutlich

FORTSETZUNG AUF SEITE 7

FORTSETZUNG VON SEITE 5

In der Logistikbranche stehen gerade österreichische Anbieter im Fokus verschiedener ausländischer Dienste oder krimineller Gruppen, die Daten abziehen oder sich für Lieferketten interessieren, denn auch geografisch ist Österreich ein wichtiger Standort.

Geréd: Vor Corona war der ganz große Cyber-Security-Trend genau der Angriff auf KMU! Wir hatten da 70-prozentige Steigerungen pro Jahr, das war sehr massiv. Und das muss ich mitbedenken, wenn ich meine Supply Chain schützen möchte, denn oft sind nicht große Unternehmen die prime targets von Kriminellen, sondern kleine Firmen, die etwa spezielle Nischenmärkte physisch oder softwaretechnisch bedienen und ganz gezielt angegriffen werden. Dabei sollte einem schon allein die breite Masse der Attacken zu denken geben.

Linhart: Einer unserer Kunden, ein klassisches KMU, das sehr spezielle Produkte für die gehobene Automobilindustrie herstellt, wurde aufgefordert, die entsprechenden Konzernrichtlinien im Datenverkehr einzusetzen – und war zuerst einmal dementsprechend überfordert. Spannend, wie das Diktat der großen Player hier auch kleine spezialisierte Unternehmen trifft, die eben über keinen eigenen IT-Officer etc. verfügen.

Geréd: Das ist der Klassiker! Wenn es Kriminellen gelingt, Luxusartikel hardwaretechnisch zu manipulieren – und dazu muss man eigentlich nur die Supply Chain kennen –, dann landet das Produkt am Ende des Tages auf jedem Fall bei jemandem, von dem Geld zu holen ist!

Glade: Ich möchte nochmals zu den Daten und Schwellenwerten zurückgehen, denn es ist wichtig, die Tipping Points, also Schwellenwerte, ab denen Systeme dann anders funktionieren und das Alte nicht wieder hergestellt wird, zu kennen. Ich glaube, Corona ist so ein Tipping Point. In der Logistik müssen wir daher von Change Management sprechen. Wir befinden uns in einer dynamischen Entwicklung und müssen dem als Firmen, Institutionen oder Behörden noch mehr Rechnung tragen. Wie können wir diese kontinuierlichen Veränderungen in unseren Managementstrukturen adressieren, auch im Sinne von Katastrophenschutz oder Präventionsmaßnahmen? Dieser Aspekt ist noch nicht angekommen.

Ich würde jetzt gerne zum Thema Infrastruktur überleiten, bei der die physische und die virtuelle Welt einander begegnen. Infrastruktur wird immer stärker digitalisiert und Elemente können von Ransomware angegriffen werden. Thales arbeitet zum Beispiel mit den ÖBB beim Aufbau einen Stellwerks in der Cloud zusammen. Wie vermeidet man hier Angriffe, etwa auch bei einem Blackout?

„Es ist wichtig, die Tipping Points, also Schwellenwerte, ab denen Systeme dann anders funktionieren und das Alte nicht wieder hergestellt wird, zu kennen. Ich glaube, Corona ist so ein Tipping Point. In der Logistik müssen wir daher von Change Management sprechen", erklärt Thomas Glade

Linhart: Hier geht es stark um Identität, egal ob es sich dabei um einen Menschen, eine Maschine oder ein Auto handelt – im Fall des Thales-Stellwerks in der Cloud vielleicht sogar um ein Außenelement, das eine Identität besitzt. In der digitalen Welt ist eine Maschinenidentität zumeist mit einem Zertifikat verbunden. Damit steht und fällt vieles mit der Qualität dieses Zertifikats, das entsprechend signiert sein muss, damit es zweifelsfrei als eigenes identifiziert werden kann. Das kann ich nur mit einer vertrauenswürdigen Infrastruktur im Hintergrund, die mit entsprechenden Hardware-Security-Modulen geschützt wird, bei der sich Schlüssel, die Signaturen oder andere Aktionen ausführen, ausschließlich in diesen Systemen befinden und nur dann benutzt werden können, wenn das Unternehmen die Berechtigung erteilt hat. Deshalb ist es enorm wichtig, dass die gesamte Chain von der Identität bis zum Backend inklusive der Kommunikation entsprechend geschützt sein muss. Das macht Thales seit Jahrzehnten und dafür bieten wir Lösungen an.

Wenisch: Zur Vermeidung von Schäden aus Blackouts oder Ransomware etc. sind bewährte und bestehende Konzepte wie Business Continuity und Business Recovery wichtig, um die Betriebsstabilität hochzuhalten. Der Faktor Mensch und das Thema Leadership spielen hier ebenfalls eine Rolle, denn ich muss auch aufgrund eines Gefühls oder einer Intuition richtige Maßnahmen setzen können. In Österreich haben wir bereits solche Gefahren abgewehrt – der Faktor Mensch bleibt ein wichtiger Schlüssel in der Arbeit mit komplexen Systemen und riesigen Datenmengen.

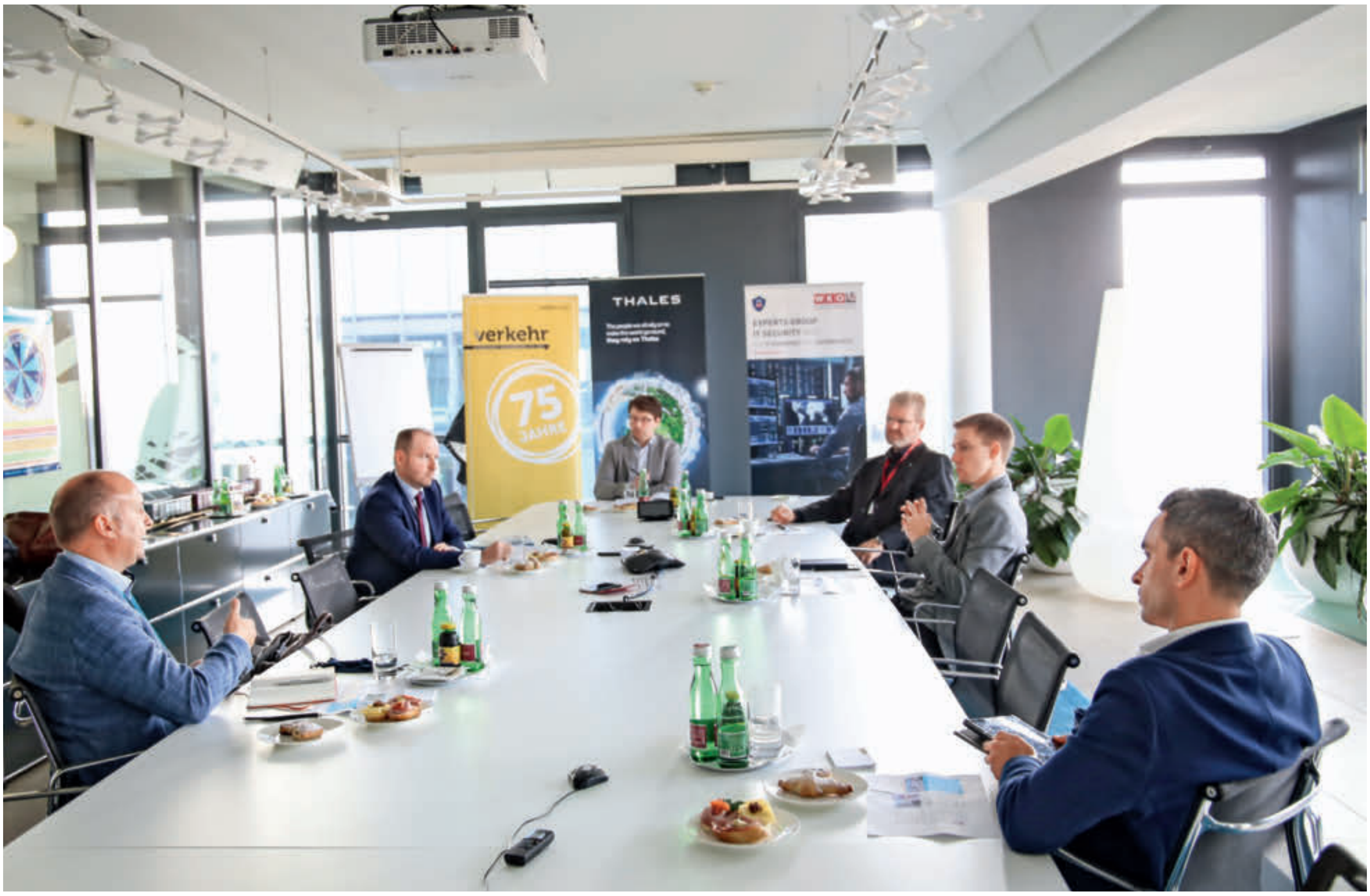
Geréd: Mit Mitarbeiter-Schulungen einerseits sowie dem Appell an die Mitarbeiter, „traut euch nachzufragen", passieren Erfolgsgeschichten, wie Cyberangriffe tatsächlich abgefangen werden können. Bei einem Cyberangriff passieren die ersten drei klassischen Schritte außerhalb der eigenen IT-Infrastruktur: Zuerst wird mit mehr oder weniger Aufwand überwacht, dann der Payload erstellt und in die hübschen Dateien gepackt, welche die Mitarbeiter dann abrufen können, klassischerweise E-Mails – oder es werden Websiten verseucht, die einzelne Personen regelmäßig besuchen. Dort, wo der nächste Schritt verhindert werden kann, nämlich in der konkreten Reaktion auf eine E-Mail – setzt Prävention an, denn gerade das Fragen-Dürfen kann im Zweifelsfall Schlimmeres verhindern. Die IT-Abteilung eines Mandanten hat beispielsweise eigens Leute dafür abgestellt, nur dafür kontaktiert zu werden, ob etwa eine E-Mail echt ist.

Glade: Redundanz ist dafür sicher das A und O: Der Plan B oder C sowie klare Kommunikationsketten, auch bei einem Stromausfall, denn jene Tage im Jahr, wo keine kritischen Situationen im Stromnetz auftreten, sind mittlerweile eher die Ausnahme. Wir müssen genau wissen, welche Optionen wir in so einem Fall noch wie lange haben und entsprechende Handlungs- und Kommunikationsketten festlegen und dann in der Prävention durchspielen. Kommunikationsketten, die im Normalfall etabliert sind, mögen im Falle eines Blackouts gar nicht mehr funktionieren und ändern sich selbstverständlich auch mit der Dauer des Ereignisses.

Abschließende Frage: Wie kann national, europaweit oder auch seitens der Unternehmen vorgebeugt werden, um im Fall der Fälle die Kontinuität von Lieferketten zu gewährleisten?

Geréd: Man braucht dazu Experten.

FORTSETZUNG AUF SEITE 8



FORTSETZUNG VON SEITE 7

Risikoabsicherung in der Logistik mit komplexen Lieferketten können nicht einzelne Abteilungen allein erledigen. Man muss sich trauen, verschiedene Fachleute zu verschiedenen Aspekten zu Rate zu ziehen, auch hinsichtlich der unterschiedlichen Typen von Bedrohungen, und daraus im Rahmen der eigenen Ressourcen Prioritäten setzen. Für die digitale Absicherung hat sich im Zuge der Pandemie wahnsinnig viel verändert. Es ist aber immer sinnvoll, beim Faktor Mensch zu beginnen, weil gut geschulte Mitarbeiter die erste Verteidigungslinie gegen Cyberrisiken sind.

Glade: Ich sehe verschiedene Aspekte: faktenbasierte Entscheidungen, Risikoprävention in einer komplexen Welt mit dynamischen Systemen und ganzheitliche Betrachtung.

Linhart: Ich würde mir konkretere Richtlinien vom Gesetzgeber wünschen, die den Unternehmen die Umsetzung ihrer Maßnahmen erleichtern. Der Faktor Mensch ist ein wesentlicher Punkt. Auch hier wären spezielle Programme seitens der Regierung positiv, um den KMU zu helfen. Auch die angesprochene Hotline der WKÖ halte ich für eine tolle Einrichtung. Ansonsten sind wir mit den Computer Emergency Response Teams (CERT) in Österreich im internationalen Vergleich recht gut ausgestattet. Und natürlich würde ich mir wünschen, dass mehr verschlüsselt wird!

> *„ES IST ABER IMMER SINNVOLL, BEIM FAKTOR MENSCH ZU BEGINNEN, WEIL GUT GESCHULTE MITARBEITER DIE ERSTE VERTEIDIGUNGSLINIE GEGEN CYBER-RISIKEN SIND" – ÁRPÁD GERÉD*

Nitschinger: Ich sehe die Verantwortung zur Steigerung der Resilienz der Lieferketten primär bei Unternehmen sowie beim Staat, wenn es um die kritische Versorgung im medizinischen oder pharmazeutischen Bereich geht. Aus meiner Sicht müssen auch KMU bewusst diese Verantwortung wahrnehmen, nämlich Risikomanagement nicht nur in der Theorie, sondern tatsächlich in der Praxis zu leben. Nicht die Checkliste in der Schublade, sondern die proaktive Auseinandersetzung ist wichtig. Ich glaube, das ist seit Corona angekommen.

Wenisch: Ich möchte drei Punkte in meinem Statement zusammenfassen: Einerseits die Prävention, zu der auch das Thema Strafverfolgung gehört, indem Anzeigen für Cyberdelikte erleichtert werden, sowie eine Erhöhung des Strafrahmens für Cyberkriminalität, denn da sind wir im internationalen Vergleich zu moderat. Der zweite Punkt, um Resilienz politisch zu unterstützen, ist die Einbeziehung von externen Expertengruppen, die fachlich fundiert und neutral entscheiden. Und schließlich braucht es meiner Meinung nach die gezielte Unterstützung von Investitionen in Unternehmen.

Vielen Dank für das Gespräch!

RESÜMEE DES ROUNDTABLES

In einer zunehmend digitalisierten und globalisierten Welt spielen virtuelle Bedrohungen eine immer größere Rolle. Dies betrifft direkt die IT von Unternehmen selbst wie auch die Logistik, deren bereits stark optimierte Lieferketten sich als besonders vulnerabel herausgestellt haben. Hochkomplexe Supply Chains können enorme Schäden aufgrund von gezielten Angriffen erleiden und generieren. Auch der Schutz kritischer Infrastruktur hat in diesem Zusammenhang höchste Priorität. Cybercrime-Delikte – sei es Erpressung, Spionage oder die Manipulation von Unternehmensdaten – dürften weiterhin massiv zunehmen, vor allem bei schlecht geschützten KMU. Vernachlässigte Sicherheitslösungen im Access-Management bei Firmennetzwerken entpuppten sich im Zusammenspiel mit Homeoffice zu einem gewaltigen Sicherheitsproblem für Firmen und Institutionen. Als direkte Folge der Covid-Pandemie hat sich das kritische Bewusstsein in den Wirtschaftsbetrieben mittlerweile nach Meinung der Experten zumindest deutlich erhöht.

Dass die strikte Einhaltung rigider Compliance-Vorschriften selbst in vergleichsweise kleinen Unternehmen eine systemrelevante Rolle haben kann, mag anfangs überraschen. Als Teil großer Lieferketten verfügen jedoch gerade KMU über einen gewaltigen Impact, so dass Kriminelle besonders leichtes Spiel haben bzw. ganz ungeahnte Möglichkeiten ausnützen können. Deutlich wird: Ohne moderne IT-technische Ausstattung können Supply Chains gar nicht mehr compliant bedient werden und auch rechtliche Fragen sind bereits eng mit IT-Sicherheitslösungen verknüpft.

Neben der frühzeitigen Erkennung problematischer Entwicklungen entlang der Supply Chains, bei Lieferanten oder im eigenen System sowie ganz besonders im Katastrophenfall spielt die theoretische und praktische Schulung der Mitarbeiter eine ganz zentrale Rolle. Gelebte Prävention muss im Bedarfsfall sofort und unvorbereitet direkt anwendbar sein. Dazu können reale Übungen im Sinne eines Planspiels und der daraus resultierenden Erkenntnisse zur Optimierung von Kommunikationslinien und vorgegebenen Abläufen einen enormen Beitrag leisten. Gerade ungewohnte Verhaltensweisen und Entscheidungssituationen wollen real geübt sein, empfiehlt der Krisenspezialist. Auch die gesicherte und an mehreren Stellen abrufbare Lagerung von Unternehmensdaten kann sich vor allem nach einem Angriff als immanent für die Betriebskontinuität herausstellen.

Von der Politik und Administration wünscht man sich klarere und präzisere Vorgaben sowie eine härtere Bestrafung bei Cyberdelikten, deren Strafmaß bisher oft in keinem Verhältnis zu dem entstandenen Schaden für das Unternehmen – oder dem Gewinn für die Kriminellen bzw. auch für die Konkurrenz – stehen.