„Cyberabwehrkonferenz Schleswig-Holstein" im Kieler Innovations- und Technologiezentrum GmbH Kiel (Freitag, 17. Juni 2022)

„Wenn Du so eine Attacke erlebst, bekommst Du Existenzangst“

Cyberabwehrkonferenz des Wirtschaftsrates Schleswig-Holstein bringt Experten und Unternehmer zusammen – 88 Prozent aller Firmen werden attackiert

Von Holger Hartwig (Agentur Hartwig3c, Hamburg)

KIEL *Es war die Zahl des Tages bei der Cyberabwehrkonferenz Schleswig-Holstein, zu der der Wirtschaftsrat der CDU e.V. nach Kiel in das Technologiezentrum eingeladen hat. 2021 sind in Deutschland durch Cyberkriminalität in der Wirtschaft Schäden mit einer Höhe von 233 Milliarden Euro verursacht worden. Grund genug, dass sich im Kieler Innovations- und Technologiezentrum GmbH fünfzig Experten und Interessierte trafen, um aktuelle Entwicklungen, die Maßnahmen seitens der Politik und der Polizei sowie Erfahrungen aus der Wirtschaft zu berichten.*

Diana Pabst, Vorsitzende der Fachkommission Digitalisierung des Wirtschaftsrates Schleswig-Holstein, machte zu Beginn deutlich, dass es „nicht mehr nur die großen Konzerne in Deutschland sind, die durch kriminelle Hacker-Gruppen angegriffen werden, sondern auch immer mehr Handwerksbetriebe, Kanzleien oder Arztpraxen“. Die größte Gefahr sei derzeit, dass die Daten der Unternehmen durch die Kriminellen verschlüsselt werden und dann erst nach der Zahlung von Lösegeld wieder freigegeben werden. Ein weiterer Trend sei, dass immer häufiger mit professionell erstellten falschen Identitäten gearbeitet werden. Pabst: „Die Zahl der Angriffe steigt von Jahr zu Jahr. Die Aufklärungsquote ist heute bisher sehr gering. Für jedes Unternehmen stellt sich die Frage, wie im Falle eines Angriffs mit dem Thema intern und extern umgegangen wird und wie sich der Schaden reduzieren lässt.“ Pabst freute sich, dass es mit der Auswahl der Referenten gelungen sei, aus verschiedenen Perspektiven auf das Thema zu schauen: Unternehmer, IT-Experten sowie Vertreter der Polizei, eines Versicherungsunternehmens und eines Wirtschaftsverbandes machten deutlich, wie komplex die Herausforderung ist.

Basler: Brutalste Erfahrung meines Unternehmerlebens

Gleich der erste Referent, **Norbert Basler** (Aufsichtsratsvorsitzender Basler AG, Ahrensburg), zeigte auf, wie schnell es gehen kann, Opfer zu werden und wie gravierend die Auswirkungen sind. Sein börsenorientiertes Unternehmen mit etwa 1000 Mitarbeitenden auf der gesamten Welt, sei nachts angegriffen worden. 1000 Server und 3000 Rechner seien betroffen gewesen. „Der Angriff kam aus St. Petersburg von einer der dort geschätzt 60 weltweit tätigen Gruppen. Das Ziel war klar: Mit Ransomware verschlüsseln, klauen und zerstören.“ Sein Unternehmen habe Glück im Unglück gehabt, weil es noch eine Sicherheitskopie gab, die nicht „gekapert“ wurde. Trotzdem habe man zwei Wochen nicht produzieren und acht Wochen im Bereich Forschung und Entwicklung nicht arbeiten können. Basler: „Wenn Du so eine Attacke erlebst, dann bekommst Du Existenzangst und suchst aus einem Ohnmachtsgefühl heraus nach Hilfe. Das war eine der brutalsten Erfahrungen meines Lebens.“

Polizei „glänzt“ mit Formularen und durch Abwesenheit

Das Glück seines Unternehmens sei gewesen, dass „wir eine sehr gute Versicherung haben, die innerhalb weniger Stunden mit einem Team anrückte und aus den Niederlanden viele Aufgaben, z.B. auch die Kommunikation mit den Erpressern, übernommen haben.“ Das seien Profis gewesen, die genau wussten, was sie machen. Basler: „Ich empfehle jedem Unternehmer, sich bei Abschluss einer Versicherung anzusehen, wie im Schadensfall reagiert wird. Die Profis haben sehr schnell viel auf den Weg gebracht.“ Während er bei der Versicherung gute Erfahrung gemacht habe, sei es bei den deutschen Behörden vollkommen anders gewesen. „Ich habe um 8 Uhr das erste Mal versucht, mit der Zentrale Ansprechstelle Cybercrime (ZAK) in Schleswig-Holstein zu telefonieren. Da ging der Anrufbeantworter ran. Man sei nur von 9 bis 15 Uhr erreichbar. Als ich dann jemanden erreicht habe, hieß es: Wir schicken Ihnen per Post einige Formulare zum Ausfüllen.“ Er habe in der gesamten Zeit keinen Beamten in seinem Haus gesehen. „Entschlossenes Handeln und Expertenwissen sieht anders aus. Da hat man uns im Stich gelassen und ich würde auch sagen, dass es keine Chance gab, uns zu helfen“, so Baslers Fazit.

Neben der Frage, wie das Unternehmen wieder ins Laufen komme, seien auch Themen wie Kundenkommunikation, Kontakt zu den Mitarbeitern und Medienarbeit wichtig gewesen. „Der einzige Rechner, der zunächst noch lief, war meiner mit einem anderen Betriebssystem. Durch die Profis und das Engagement aller Mitarbeiter kann ich sagen: Es hätte schlechter laufen können.“ Entscheidend sei, im Fall der Fälle durch die Versicherung absolute Profis sehr schnell an seiner Seite zu haben.

Wilke: Manchmal reicht selbst ein doppelter Boden nicht

Von einer Erfahrung, die im Zusammenhang mit dem Ukraine-Krieg, steht, berichtete **Utz Wilke** (Geschäftsführender Gesellschafter, Filiago GmbH & Co. KG, Bad Segeberg). Er bietet seit 2003 Satellitendienste für Unternehmen an, die über diese Technik anstelle der Festnetz- oder Mobilfunkverbindung Daten austauschen. Wilke: „Katastrophen kommen schneller als man denkt und man kann sich nicht zu 100 Prozent schützen. Uns hat es eine halbe Stunde bevor Russland den Ukraine-Krieg begonnen hat erwischt. Einige unserer Kunden waren nicht mehr handlungsfähig.“ Was war passiert? Zehntausende Anlagen bzw. Modems von Kunden, die europaweit über einen Satelliten kommunizieren und zum Zeitpunkt des Angriffs online waren, wurden durch das Aufspielen neuer Software zerstört. Wilke: „Bei uns hat es nur einen kleinen Teil der Kunden betroffen. Insgesamt hat es 15 Tage gedauert, bis das System wieder lief.“ Größtes Opfer dieser Attacke sei das Unternehmen Enercon gewesen, das Windkraftanlagen nicht mehr wie gewünscht steuern konnte.

Ziel des Angriffs sei Osteuropa gewesen. Wilke: „Für uns stellte sich die Frage, warum ein ziviles Netzwerk angegriffen wurde. Dann hat sich herausgestellt, dass ein Partner aus der Ukraine die Dienste an das ukrainische Militär verkauft hat. Damit hatte niemand gerechnet“. Aus Wilkes Sicht ist die Verletzbarkeit eines IT-Systems nicht vorhersehbar. „Wer sich schützen will, der braucht doppelte Backups bei den Zugangsdaten, der Energieversorgung und der Datenleitung.“ Es sei wichtig, sich in diesen Fragen immer von IT-Spezialisten beraten zu lassen. „Manchmal reicht auch ein doppelter Boden nicht, sondern es braucht einen dritten oder vierten Boden.“ Bei dem beschriebenen Angriff seien die Kunden am schnellsten wieder arbeitsfähig gewesen, die ein Ersatz-Modem vor Ort hatten.

Weingarten: Wir haben eine Cybersicherheitskrise höchster Stufe
Sehr deutliche Worte formulierte auch **Bert Weingarten** (Vorstand der PAN AMP AG, Hamburg). Er skizzierte Markt- und Systembeobachtungen eines Sicherheitsdienstleisters und beendete seine Ausführung zu den Möglichkeiten, wie heute Deep-Fake-Attacken mit gefälschten Audio- und Videonachrichten umgesetzt werden, mit den Worten: „Ich denke, ich habe Sie genug verunsichert."

Weingarten, der sich seit vielen Jahren mit seinem Unternehmen mit dem Thema Sicherheit von Daten und Angriffen auch auf mobile Devices beschäftigt, konzentrierte sich auf die Frage, wie es heute möglich ist, menschliche Kommunikation perfekt digital und realitätsnach zu erzeugen. Weingarten machte deutlich, dass es für Täter, die menschliche Profile erzeugen wollen, trival sei, an Daten zu kommen. Innerhalb von drei bis sechs Monaten könnten Menschen so mit ihrer Persönlichkeit, Stimme und Abbild ausgeforscht werden, dass dann „alles möglich ist." Dafür würden Telefonate, Audio-Nachrichten, Videos oder Videokonferenzen gezielt ausgewertet. Weingarten: „Aus diesen Telemetrie-Daten werden dann Botschaften entwickelt, die beispielsweise eine Assistentin veranlassen, 60 Millionen Euro auf ein Konto zu überweisen, weil sie der festen Überzeugung ist, diese Anweisung von ihrem Chef erhalten zu haben." Diana Pabst empfahl dazu die Verabredung von Kodewörtern mit den Mitarbeitern.

Neuer Umgang erforderlich, da alles „perfekt fakebar ist"
Weingarten ging in diesem Zusammenhang auf die Datenschutzrichtlinien der weltweit führenden Anbieter von Videokonferenzsystem ein. „Mit der Begründung der Qualitätsverbesserung sichern sich alle Anbieter das Recht zu, alle Konferenzen aufzuzeichnen und – nicht EU-konform, die Anbieter sitzen ausschließlich in den USA - auswerten zu dürfen." Wer das über die Softwareeinstellungen ablehne, der müsse mit Funktionseinschränkungen leben. Zu den Möglichkeiten einer kriminellen Nutzung entgegenzuwirken, sagte Weingarten trocken: „Diese Kapazitäten haben die Landeskriminalämter aktuell nicht." Er gehe davon aus, dass es in den nächsten Jahren ein substanzielles Problem wird, „weil man nicht mehr weiß, wer was sagt." Er empfehle, den Gesprächspartner künftig immer in Frage zu stellen und „Quellen stärker auf Zweit- oder Drittmeinung zu verifizieren". Man werde mit dem Thema komplett anders umgehen müssen. „Alles ist perfekt fakebar."

Wagemann: 88 Prozent aller Firmen werden attackiert
Wie die Wirtschaft und der Gesetzgeber auf die Zunahme der Angriffe reagieren könnten, dazu referierte Markus Wagemann, Geschäftsführer der Allianz für Sicherheit in der Wirtschaft Norddeutschland (ASW). Es zeige sich, dass bereits jetzt 88 Prozent aller Unternehmen angegriffen würden, beispielsweise auch durch Mail mit schadhaften Anhängen. „Ich höre immer: Ja, ich weiß, dass es da Gefahren gibt. Aber mich wird das nicht betreffen. Nur jeder dritte Firmenchef meint, dass es ihn auch treffen könnte. Dabei ist mittlerweile kein Unternehmen mehr sicher", so Wagemann. Er regte an, dass der Gesetzgeber – ähnlich wie beim Thema Brandschutz – eine Vorgabe über das Arbeitsschutzgesetz machen sollte, dass Mitarbeitende regelmäßig für den Umgang mit IT-Gefahren unterwiesen werden. Zweimal pro Jahr sollte ein Überblick über die Methoden der Kriminalität gegeben und die Fähigkeiten, sich vor Angriffe zu schützen, geschult werden. Zudem sollten Notfallpläne zur Pflicht werden. Wagemann: „Ich bin überzeugt, dass die Mitarbeitenden bei diesen Schulungen mitmachen, denn sie hätten ja auch im Privatbereich einen Nutzen davon." Wichtig sei, dass bei der Gesetzgebung keine Überregulierung stattfinde und die Kostenseite berücksichtigt werde.

Podzins: Versicherungen werden deutlich teurer werden
Wie sich Firmen gegen die Schäden absichern können und was eine Cyberversicherung kostet, darüber informierte **Hauke Podzins** (Versicherungsmakler Podzins GmbH & Co. KG, Kaltenkirchen) anhand der fiktiven Firma Maschinenbau SH. Das Unternehmen hat 110 Mitarbeitende und 20 Mio. Euro Jahresumsatz und ist in der Verwaltung, der Logistik und der Produktion digital vernetzt.

Podzins machte deutlich, dass die meisten Schäden durch falsches oder unbewusstes Verhalten von Mitarbeitenden entstehen. „Bei kleineren Firmen steht meistens der technische Schutz im Vordergrund. In fast 60 Prozent sind Mitarbeitende und ihr Verhalten der Grund für den Erfolg der Angreifer“, so der 28-Jährige. Die Cyberversicherung unterscheide sich von den meisten anderen Versicherungsarten dadurch, dass der Versicherer Kompensation bzw. Reduzierung des Schadens für das Unternehmen oder für Dritte durch professionelle Hilfe und Analyse der Umstände direkt eingreift. Zudem werde bei Abschluss einer Police und dann regelmäßig auch eine Analyse der Gefahren zur Erhöhung der Resilienz vorgenommen. Aktuell gebe es in Deutschland etwa 40 Anbieter für diesen Versicherungstyp und „jeder hat für die Versicherungsleistung sein Baukastensystem“. Aktuell müsste ein Handwerksbetrieb wie die Maschinenbau SH mit jährlichen Versicherungskosten von etwa 1000 Euro rechnen. Für Steuerberater oder Arztpraxen werde der Schutz aktuell für etwa 500 Euro pro Jahr angeboten. Podzins: „Es ist allerdings davon auszugehen, dass die Absicherung tendenziell in den nächsten Jahren deutlich teurer wird und sich die Bedingungen weiterentwickeln werden.“ So sei nicht klar, wie geregelt werde, wenn ein Angriff im Zuge eines Krieges gezielt durch ein anderes Land erfolge.

Röhrl: Vertraulichkeit, Verfügbarkeit und Verlässlichkeit sichern
Während der Konferenz kamen auch Vertreter der Polizei und des Landes Schleswig-Holstein zu Wort. Sie hatten angesichts der geschilderten Erfahrungen aus der Wirtschaft einen schweren Stand. **Peter Röhrl** (Informationssicherheitsbeauftragter für die Landesverwaltung Digitalisierung und zentrales IT-Management der Landesregierung) machte deutlich, dass aus Sicht des Landes die Informationssicherheit im Fokus stehe. Es gehe neben der Cybersicherheit um die Frage, wie im Zuge der Demokratie und Rechtsstaatlichkeit sichergestellt werden kann, wie - so wie in der analogen Welt - ein Schutz der Vertraulichkeit, eine Verfügbarkeit und Verlässlichkeit von Infos und deren Verarbeitung gewährleistet werden kann. Das Land setzte auf die Handlungsfelder Prävention, Detektion, und Reaktion. Dabei komme es auf eine gute Verzahnung der drei Säulen Strafverfolgung (Landes- und Bundeskriminalamt), Informations- und Cybersicherheit (Bundesamt für Sicherheit in der Informationstechnik und Wirtschaftsschutz (Bundesamt für Verfassungsschutz) an. „Digitale Resilienz ist eine gesamtstaatliche Aufgabe. Der Fokus muss auf der Widerstandsfähigkeit einschließlich der Notfallplanung liegen. Dabei spielen auch die Unternehmen eine wichtige Rolle.“

Oeffner: Kein Blaulicht und keine Hardware-Beschlagnahmung
Für **Lars Oeffner** (Dezernatsleiter Cybercrime und Digitale Spuren Landeskriminalamt Schleswig-Holstein, Kiel) ging es darum, Vertrauen zurückzugewinnen und die Unternehmen zu ermuntern, bei Angriffen immer die Polizei mit an den Tisch zu holen. Oeffner: „Als erstes entschuldige ich mich bei Herrn Basler. Das ist absolut nicht gut gelaufen. Die Zentrale Ansprechstelle Cybercrime habe sich weiterentwickelt. Heute würde die Reaktion auf den Anruf anders

ausfallen.“ Oeffner machte deutlich, dass die Zahl der Angriffe, die der Polizei gemeldet wurden, in Schleswig-Holstein zuletzt sehr stark und über dem Bundesdurchschnitt angestiegen sei. Leider könne er das über die Aufklärungsquote nicht sagen, aber „das liegt auch daran, dass 95 Prozent der Täter aus dem Ausland kommen.“ Bei Cybercrime sei man bei einer Quote von 30 Prozent, bei Ransomware bei lediglich zwei Prozent. Trotz dieser Zahlen ermunterte Oeffner die Teilnehmer der Konferenz, die Polizei immer mit an den Tisch zu holen. „Wir haben verstanden, dass es bei einem Angriff bei Ihnen brennt und wir mit unserer Ermittlungsarbeit der Täter nicht an erster Stelle stehen. Wir bringen unsere Kenntnisse ein und beraten beispielsweise im Umgang mit den Tätern.“ Für die Ermittler sei es dabei selbstverständlich, „nicht mit Blaulicht zu kommen, auch nicht im Unternehmen nach anderen Informationen oder Straftaten zu schnüffeln, Hardware zu beschlagnahmen oder die Handlungsfreiheit im Umgang mit Erpressern einzuschränken“. Er machte deutlich, dass nur die Einbindung der Ermittler dafür sorgen könne, dass „wir mehr Täter zur Rechenschaft ziehen können, denn nur dann gibt es keine Lösegelder mehr und die Fallzahl steigt nicht weiter“.

Bildunterschrift:
Sie sorgten für den Blick auf die steigende Kriminalität im IT-Bereich für verschiedene Blickwinkel: die Referenten des Cyberabwehrkonferenz des Wirtschaftsrates Schleswig-Holstein des Wirtschaftsrates mit Daniela Pabst, Vorsitzende der Fachkommission Digitalisierung (links), und der Landtagsabgeordneten Birte Glißmann (rechts).

Foto: Hartwig3c