

Datum: 18.03.2023

☒ Jeverisches Wochenblatt

☐ Nordwest-Zeitung

☒ Guten Morgen Sonntag

☐ Wilhelmshavener Zeitung

☐ Anzeiger Harlingerland

☐

Polizeidirektor geht mit Medien hart ins Gericht

SICHERHEIT Heiko von Deetzen über Kriminalität, Sensationslust und Automaten Sprenger – Vortrag beim Unternehmerfrühstück

VON JÖRG STUTZ

JEVER – Genaue Zahlen nannte Heiko von Deetzen, Leiter der Polizeiinspektion Friesland/Wilhelmshaven, nicht. Was die Kriminalitätsrate im Landkreis angeht, konnte der Polizeidirektor die Teilnehmer des Volksbank-Unternehmerfrühstücks beruhigen: „In Friesland ist die Welt noch in Ordnung.“ Anders als mit der tatsächlichen Bedrohung durch Kriminalität sieht es mit der subjektiven Sicherheit aus: Wie sehr fühlt sich der Bürger von Gängen, Gangstern und Gewalttätern bedroht?

Beispiel Impfskandal

Bei der Beantwortung ging von Deetzen im Immobilien- und Finanzzentrum der Volksbank Jever mit den Medien hart ins Gericht. „Da wird gelogen, dass sich die Balken biegen“, so der Gastredner, der vor allem sozialen Medien vorwarf, die

„Sensationslust der Bürger“ befriedigen zu wollen. Wohin das führt, zeigte er am Beispiel des „Impfskandals“ im Impfzentrum Roffhausen – nach Ansicht des 60-jährigen „eine Körperverletzung, wie sie in Deutschland täglich tausendfach passiert“. Von Deetzen, der von 2004 bis 2008 das Kommissariat in Jever leitete, ist sich sicher: Unter anderen Umständen – ohne mediale Aufmerksamkeit – hätte die Staatsanwaltschaft das Verfahren eingestellt. Zur Erinnerung: Einer 40-jährigen Krankenschwester war vorgeworfen worden, im April 2021 in sechs Fällen Corona-Impfstoff gegen eine Kochsalzlösung ausgetauscht zu haben.

Doch die öffentliche Empörung ist auch schnell wieder vorbei. So ist von Deetzen überzeugt: Die derzeitige Diskussion nach dem jüngsten Amoklauf in Hamburg über eine Verschärfung des Waffenrechts „verebbt in zwei Wochen wieder“. Um die „emotionale Welle

im Netz“ zu verhindern, setzt die Polizei auf eine verstärkte Öffentlichkeitsarbeit. Ziel sei es, so von Deetzen, „die Hohheit in der Berichterstattung“ wiederzugewinnen.

Reichsbürger

Zum Thema Reichsbürger und Querdenker: Diesen Personenkreis habe es schon immer gegeben. Jedoch habe die Pandemie für beide Gruppen eine andere Plattform geschaffen, um den „Blödsinn“ zu veröffentlichen. „Die kommen auf Ideen, das ist sagenhaft“, sagte von Deetzen mit Blick auf die kruden Inhalte, mit der auch seine Kollegen immer wieder konfrontiert würden. Dabei sind seiner Einschätzung nach die Reichsbürger- und Querdenker-Gruppen noch so klein, dass sie keine Gefahr für die Demokratie darstellen.

Zu einem Geschäftsmodell habe sich das Sprengen von Geldautomaten entwickelt. Die

Tätergruppen – oft aus Belgien und den Niederlanden – mieten PS-starke Autos an, montieren gestohlene Nummernschilder, sprengen in Deutschland Geldautomaten in die Luft und flüchten mit Höchstgeschwindigkeit. Von Deetzen warb um Verständnis dafür, dass sich die Polizei unter diesen Umständen mit den Flüchtenden keine Verfolgungsfahrten liefere: Das bringe die Kollegen und andere Verkehrsteilnehmer in Gefahr. Bei der Aufklärung der Straftaten werde die Polizei trotzdem „zunehmend erfolgreicher“.

Der Gastredner warb dafür, den Zugang zu Geldautomaten in der Zeit von 21 bis 6 Uhr zu verwehren. Denn: Beschränkte Öffnungszeiten nehmen den Banden schlichtweg die Möglichkeiten. Weil die Automaten Sprenger auch mit Festsprengstoffen – teils ganze Häuser in die Luft fliegen lassen, ist es für von Deetzen nur eine Frage der Zeit, wann auch Menschen zu Schaden kommen.



Heiko von Deetzen, Leiter der Polizeiinspektion, mahnt Zurückhaltung der Medien an.

BILD: JÖRG STUTZ

Datum: 16.03.2023

☐ Jeverisches Wochenblatt

☒ Nordwest-Zeitung

☐ Guten Morgen Sonntag

☐ Wilhelmshavener Zeitung

☐ Anzeiger Harlingerland

☐

„Moderner Cyberkrimineller ist der Ultra-Kapitalist“

VORTRAG Experte gibt Tipps zu Sicherheit vor Hackerangriffen

VON SAROM SIEBENHAAR

JEVER – „Es gibt zwei Unternehmen. Die, die einen Angriff hatten und jene, die einen hatten, es aber nicht bemerkt haben“, sagt Frank Marquardt von der Volksbank Jever. Damit leitet er das Unternehmerfrühstück ein, bei dem es um Cyberkriminalität und Cybersicherheit geht. Nils Traß, Kriminalhauptkommissar mit dem Schwerpunkt Cybercrime, gibt Tipps, wie sich Unternehmen besser vor Hackerangriffen schützen können.

Vor-Ort-Infektion

„Das Elend der Welt liegt im deutschen Mittelstand“, sagt er. „Denn das ist das attraktivste Ziel für Cyberkriminelle.“ Die Unternehmen seien groß genug, um lukrativ zu sein und klein genug, um sich nicht richtig vor Angriffen schützen zu können. Aber welche Ressourcen sind für Cyberkriminelle interessant? Über E-Mails können Hacker

Daten gewinnen und weiterverkaufen. Server können gekapert und für Preise von 1.500 bis 2.000 Euro vermietet werden. „Die Käufer nutzen diese dann für illegale Downloads oder Kinderpornografie“, sagt der Experte. Geschäftsgeheimnisse dienen den Kriminellen entweder als Erpressungsgrundlage oder Handelsware.

Vor allem der „Faktor Mensch“ stelle eine große Sicherheitslücke dar. „Das finde ich schon besonders, wie sehr dieser Faktor zum Problem werden kann, oft ja auch ungewollt“, sagt Bastian Lockmann, Geschäftsführer des Bauunternehmens Heino Frerichs aus Jever. Die Entwicklung im Bereich „Vor-Ort-Infektion“ sollte allen Unternehmen ebenfalls zu Denken geben, so Traß. „Das können Reinigungskräfte, Paketzusteller oder andere Leute sein“, erklärt er. Der physische Zugriff auf das System sei nicht zu unterschätzen. „Ein USB-Stick mit spezieller Funktion reicht und die Täter



Für Cybersicherheit (von links): Frank Marquardt (Volksbank Jever); Nils Traß, Kriminalhauptkommissar; Michael Engelbrecht, Vorsitzender Volksbank Jever, und Heiko von Deetzen, Polizeidirektor Wilhelmshaven/Friesland. BILD: SIEBENHAAR

haben vollen Zugriff“

Und was hilft gegen Cyberangriffe? „Hilfreich ist eine Vernetzung der Sicherheitssysteme, dass diese sich gegenseitig alarmieren“, sagt Traß. „IT-Sicherheit muss Chefsache sein“, betont er und nimmt dabei die Unternehmer in die Pflicht. Außerdem notwendig: Zusatzverschlüsselungen, ein deckendes Update-System und eine aktive Netzwerküberwachung. Gerade der letzte Punkt sei wichtig.

„Denn die meisten Täter halten sich für einen langen Zeitraum im Netzwerk auf und beobachten“, sagt Traß. In Deutschland im Schnitt anderthalb Jahre.

Zudem empfiehlt der Experte den IT-Grundsatz des Bundesamtes für Sicherheit in der Informationstechnik (BSI). „Das sollte ausreichen.“ Aber: „100-prozentige sichere IT gibt es heutzutage nicht mehr“, sagt der 41-jährige. „Es ist mittlerweile kein ob mehr, son-

dern ein wann. Irgendwann gelingt den Tätern der Zugriff.“

Professionalität

Traß findet vor allem die zunehmende Professionalisierung gefährlich. Cyberkriminalität als Service ist das Stichwort. „Da wird Arbeitsteilung betrieben, das ist heute fast wie ein Unternehmen“, sagt er. „Der moderne Cyberkriminelle ist der Ultra-Kapitalist.“ Mittlerweile werde alles, was auf dem freien Markt funktioniert, für das Internet adaptiert und kopiert. Als Beispiel nennt er den Drogenhandel, der bereits seit langem auch im Internet stattfindet.

Die Unternehmer nehmen einiges mit aus dem Vortrag. „Wir müssen jetzt versuchen die Lücken zu finden, die man schließen muss“, sagt Andreas Buchhold vom Sanitätshaus Gebauer aus Wilhelmshaven. Christian Ressel vom IT-Dienstleister EDV-Crew ist vor allem der Risikofaktor Mensch im Gedächtnis geblieben.

Mittelstand steht im Fokus von Cyberangriffen

KRIMINALITÄT IT-Fachmann gibt wichtige Tipps beim Unternehmerfrühstück

VON JÖRG STUTZ

JEVER – Die Zahlen sind eindeutig: Während im Bereich der Polizeidirektion Oldenburg im vergangenen Jahrzehnt die Gesamtzahl der Delikte um rund 14 Prozent zurückgegangen ist, gab es im gleichen Zeitraum bei der Cyberkriminalität einen Anstieg um 10,6 Prozent – und die Hauptzielgruppe der Internet-Verbrecher war am Mittwochvormittag zu Gast beim Unternehmerfrühstück der Volksbank Jever. Denn, so sagte Nils Traß, Sachbearbeiter Cybercrime bei der Polizeidirektion Oldenburg, zu den rund 50 Firmenchefs, die im Immobilien-

und Finanzzentrum zusammengekommen waren: Der deutsche Mittelstand sei „das attraktivste Angriffsfeld für Cyberkriminelle“.

Auch aus einem weiteren Grund ist dem einen oder anderen Mittelständler der Appetit auf die gereichten Schnitten vielleicht vergangen. Denn was die IT-Sicherheit in Unternehmen angeht, gibt es laut Traß keinen hundertprozentigen Schutz. „Irgendwann schafft es ein Angreifer ins System“, und das, so der Kriminalhauptkommissar, sogar bei Dienstleistern im Bereich der IT-Sicherheit.

Weil die Lokalisierung der Täter immer schwieriger wird,

„Irgendwann schafft es ein Angreifer ins System.“

Nils Traß
Sachbearbeiter Cybercrime
Polizeidirektion Oldenburg

rät der Fachmann „in eine gute Absicherung“ zu investieren. Dabei reicht nach Einschätzung des Informatikers das klassische „Festungsmodell“ aus Firewall, Virenerkennung und Backup-Systemen nicht mehr aus. Vielmehr müssten die Unternehmen auch den „menschlichen Fak-

tor“ im Blick haben. Das betrifft sowohl die eigenen Mitarbeiter als auch die „Vor-Ort-Infektion“ durch diejenigen, die in den Betrieben unerlaubt auf die Rechner zugreifen.

Traß weiß, dass Investitionen in die IT-Sicherheit nicht billig sind. Wer überlegt, ob sich die Ausgaben lohnen, sollte sich jedoch die Frage stellen: „Was kostet eine Stunde Systemausfall?“ Deshalb sein Fazit: Wenn Firmenchefs die möglichen Kosten für die IT-Sicherheit betrachten, sollten sie auch die Kosten für eine „absolut arbeitsunfähige Informationstechnik einpreisen“.

→ **JEVER, SEITE 3**

Täter forschen Firmen aus, bevor sie zuschlagen

CYBER-KRIMINALITÄT Polizeiexperte informiert beim Unternehmerfrühstück der Volksbank über Gefahr aus dem Internet

VON JÖRG STUTZ

JEVER/FRIESLAND – Den Roboterstaubsauger, die Klimaanlage, die ferngesteuerte und die intelligente Tür-Gegensprechanlage werden einige Firmenchefs jetzt mit anderen Augen betrachten. Beim Unternehmerfrühstück der Volksbank Jever erfuhren die rund 50 Teilnehmer am Mittwoch, dass auch diese elektronischen Helferlein Firmennetzwerke espionieren können. „Internet of Things“ heißt die Methode, bei der selbst Haushaltsgeräte Teil der globalen Infrastruktur sind und die, so Nils Traß, auch von Cyber-Kriminellen genutzt wird.

„Leichtere Beute“

Wie der Kriminalhauptkommissar berichtete, geraten immer stärker Firmen in den Fokus der Internet-Verbrecher. Der Sachbearbeiter Cybercrime bei der Polizeidirektion Oldenburg schätzt, dass etwa die Hälfte der Angriffe auf kleine und mittlere Betriebe zielt. Volksbank-Vorstandsvorsitzender Michael Engelbrecht berichtete, dass das Rechenzentrum der Genossenschaftsbanken im westfälischen Münster täglich tausende Cyberangriffe



Stellten das Thema Cybersicherheit in den Mittelpunkt (von links): Volksbank-Prokurist Frank Marquardt, Nils Traß, Michael Engelbrecht und Heiko von Deetzen.

abwehrt – mit Erfolg, wegen der hohen Investitionen in die IT-Sicherheit. Mittelständler seien eine „leichtere Beute“.

Jedes neue Internet-Angebot sei für Kriminelle eine „potenzielle Gelddruckmaschine“, so Traß. Demnach entsteht durch diese Art der Kriminalität derzeit weltweit ein jährlicher Schaden in Höhe von rund 1,5 Billionen US-Dollar. Während im Bereich der Polizeidirektion Oldenburg im ver-

gangenen Jahrzehnt die Zahl der Delikte um rund 14 Prozent zurückgegangen ist, gab es in dem Zeitraum bei der Cyberkriminalität ein Plus von 10,6 Prozent.

Die Täter

Traß weiß, dass viele „traditionelle Kriminelle“ in das neue Tätigkeitsgebiet abwandern. Der Informatiker sprach von „Ultrakapitalisten ohne

Moral- und Rechtsempfinden“, die oft aus dem Ausland agieren. Eine zweite Form von Internet-Gangstern macht es sogar möglich, dass auch Laien in dieses „Geschäft“ einsteigen können. Sie verkaufen Cybercrime-Komponenten inklusive „handgerecht designter“ Computerviren. Dabei gilt für beide Formen der Internet-Kriminellen, dass die Ermittlungsbehörden die Täter oft sogar mit Namen kennen, internationales

Recht die Fahndung oder das Verhaften jedoch erschwert.

Glaubt man dem Referenten, ist eine Attacke auf die Firmendaten so gut wie unausweichlich: „Die Täter gehen durch die IT-Infrastruktur ein und aus.“ Bevor die Kriminellen zuschlagen, tummeln sie sich laut Traß bis zu einerinhalb Jahren in den Systemen. „Sie werden beobachtet“, so die Schreckensvision des Beamten.

„Nicht zahlen!“

Bei den beim Vortrag vertretenen Firmen gab es bisher keine Attacken. Jedoch wusste Engelbrecht von betroffenen Firmenkunden, die für die IT-Schadensbehebung richtig tief in die Tasche greifen mussten. Traß zum Thema Cyber-Erpressung, also wenn Kriminelle ein Netzwerk lahmlegen oder wertvolle Daten stehlen: „Als Polizist würde ich sagen, nicht zahlen, aber...“ Doch, auch wenn die Erpressungsoffer zahlten, heiße das nicht, dass die Internet-Kriminellen die Daten wieder herstellen wollten – oder überhaupt können.

Der Leiter der Polizeiinspektion Wilhelmshaven/Friesland, Heiko von Setzen, sprach über das Thema „Innere Sicherheit“. Wir berichten noch.

DAS RÄT DER EXPERTE

Expertentipps:

- IT-Sicherheit muss Chefsache sein
- Krisenreaktionsteam bestimmen und Mitarbeiter-Schulungen anbieten
- Sicherheits-Software ständig auf den neuesten Stand halten
- wertvolle Dateien und Arbeitsbereiche verschlüsseln und/oder vom Hauptnetzwerk abkoppeln

Gefährdete IT-Bereiche:

- E-Mail-Server für Spam und Phishing
- Unternehmensserver als Datenserver für illegale Downloads
- die IP-Adresse für Online-Betrug
- Geschäftsgeheimnisse als Erpressungsgrundlage oder als Handelsware

Ansprechpartner:

Zentrale Ansprechstelle Cybercrime (ZAC) beim Landeskriminalamt; die Polizei vor Ort.

- www.zac-niedersachsen.de
- www.vds.de
- www.bsi.de