Cybermeister

Aus Schaden wird man klug: Im Kampf gegen die Cyberkriminalität setzt sich Dänemark an die Weltspitze.

„Öffnen Sie diese E-Mail von ‚McDonald's' nicht". Auf meinem Handy-Display poppt in weißen Buchstaben auf grünem Grund das Wort „Warnung" auf. Darunter steht – mit einem gelben „M" versehen – „*Vi er kede*", ein dänisches „Sorry". Das klingt irgendwie vertraut und lässt einen unwillkürlich an fettige Burger und Pommes denken, den sündigen Genuss nach einem langen Arbeitstag im Büro.

Mit dieser Meldung wird vor einer – als Nachricht von McDonald's getarnten – Betrugsmail gewarnt, die gerade im Umlauf ist. Versendet wurde die Warnmeldung von der dänischen App *Mit digitale selvforsvar* („Mein digitaler Selbstschutz"). Laut Projektleiterin Ulla Malling wurde die App seit ihrem Start im April 2017 bereits 250 000 mal heruntergeladen und hat durchschnittlich 80 000 aktive Nutzerinnen und Nutzer pro Monat.

Die App informiert über digitalen Betrug, Gefährdung durch Viren und Malware, Live-Updates von Banken und Strafverfolgungsbehörden und gibt sogar konkrete Ratschläge, wenn es aktuell eine Sicherheitslücke gibt. Die Initiative ist ein Gemeinschaftsprojekt des dänischen Verbraucherrats *Forbrugerrådet Tænk*, der gemeinnützigen Organisation *TrygFonden*, der Finanzwirtschaft und des dänischen Rates für Kriminalprävention *Det Kriminalpræventive råd*. Die App steht sinnbildlich für das dänische Konzept für Cyber- und Informationssicherheit mit seiner nahezu perfekten Synergie zwischen verschiedenen Institutionen sowie deren fokussierten Blick auf die alltägliche Sicherheit von Bürgerinnen und Bürgern wie auch Unternehmen.

Bis vor kurzem stand Dänemark mit seinen knapp über 5,8 Millionen Einwohnern in der öffentlichen Wahrnehmung deutlich im Schatten der Big Player der Cybersecurity-Branche wie den USA, Israel und dem Vereinigten Königreich. Doch inzwischen entfaltet das Land eine schwungvolle Dynamik, die es ins Rampenlicht rückt.

Dänemark belegt laut dem britischen Sicherheitsunternehmen Comparitech den ersten Rang unter den cybersichersten Ländern der Welt.

Dänemark belegt laut dem britischen Sicherheitsunternehmen Comparitech den ersten Rang unter den cybersichersten Ländern der Welt. Wie hat das Land das geschafft? Und könnte es damit zu tun haben, dass es sich nach der großen Cyber-Attacke von 2015/2016, die Kopenhagen auf „die Geheimdienste oder zentrale Stellen der russischen Regierung" zurückführte, um mehr Informationssicherheit bemüht hat?

Im April 2017 veröffentlichte die Kopenhagener Zeitung Berlingske einige Ergebnisse aus dem Bericht des *Center for Cyber Security* (CFCS) des dänischen Militärnachrichtendienstes. Dieser Bericht hatte aufgedeckt, dass dieselbe Hackergruppe, die 2016 hinter einem Cyberangriff auf die Server der Demokratischen Partei in den USA stand, sich Zugang zu den E-Mail-Konten ausgewählter Mitglieder des dänischen Verteidigungsministeriums verschafft hatte. Die geleakten Daten sollen zwar nicht vertraulich gewesen sein, ließen sich aber immerhin dazu nutzen, Mitarbeiter durch Erpressung als Agenten anzuwerben, so das CFCS.

Dänemarks damaliger Verteidigungsminister Claus Hjort Frederiksen stufte die Sicherheitslücke als „äußerst kritischen Sachverhalt" ein. Nach Einschätzung mehrerer Geheimdienste stand hinter dem Angriff höchstwahrscheinlich die gemeinhin mit dem russischen Militärgeheimdienst in Verbindung gebrachte Gruppe APT28, auch bekannt als „*Fancy Bear*".

Nur vier Jahre nach Bekanntwerden des Angriffs schoss Dänemark nun an die Spitze des Comparitech-Rankings. Laut Erhebungsleiterin Rebecca Moody erreichte Dänemark in zehn von fünfzehn Kategorien die höchste Punktzahl. Kein einziger Nutzer in Dänemark war von mobilen Ransomware- und Banking-Trojanern betroffen. Besonders gut schnitt Dänemark auch mit Blick auf den Anteil der von Ransomware-Trojanern (0,02 Prozent) und Kryptominern (0,11 Prozent) attackierten Nutzern ab.

Die Studie, die auf den Daten von Kaspersky Lab für das dritte Quartal 2020 basiert, befasst sich vor allem mit Malware und liefert keine genaueren Informationen zu rechtlichen und strategischen Fragen. Im Global Cybersecurity Index 2018, der diese Fragen einbezieht, rangiert Dänemark in der Region Europa mit einer Punktzahl von 0,85 auf Platz 12. Die Comparitech-Studie liefert dennoch einen Anhaltspunkt dafür, worin die Dänen besonders erfolgreich sind: in den Bereichen

individuelle digitale Hygiene und Sicherheit im Finanzdienstleistungssektor.

Letzteres ist zumindest teilweise auf den weit verbreiteten Einsatz der Zwei-Faktor-Authentifizierung (2FA) zurückzuführen. Da für alle staatlichen Online-Angebote und im Finanzsektor nur persönliche digitale Signaturen als Login verwendet werden, lassen sich mit dieser Form der Authentifizierung bestimmte Angriffswege wirksam blockieren. Ein weiterer entscheidender Faktor sind gut entwickelte Banking-Apps.

Kein einziger Nutzer in Dänemark war von mobilen Ransomware- und Banking-Trojanern betroffen.

In den nächsten Jahren will Dänemark umgerechnet mindestens 202 Millionen Euro in seine Cyber- und Informationssicherheit investieren. Laut ihrem Strategieplan für die Jahre 2018 bis 2021 stützt die Regierung sich dabei auf drei Säulen: Stärkung der technologischen Resilienz, verstärkte Aufklärung der Bürgerinnen und Bürger sowie engere Koordination zwischen den verschiedenen Akteuren. Inzwischen arbeitet Dänemark intensiv daran, die neuralgischen Punkte seiner IT-Infrastruktur zu bestimmen. Dies wird der Regierung helfen, sich mit entsprechenden Leitlinien und Strategien auf Krisenfälle vorzubereiten und Sicherheitslücken vorzubeugen.

Bedeuten diese Bemühungen also, dass Dänemark seine Hausaufgaben nach den großen IT-Sicherheitsvorfällen von 2015/2016 ordentlich erledigt hat? Während es nach Meinung des Redakteurs der Comparitech-Studie Paul Bischoff „ganz danach aussieht“, äußert Rebecca Moody sich vorsichtiger: „Wahrscheinlich schon. Wer einmal Opfer eines erfolgreichen Cyberangriffs wurde, ist eher bereit, seine Betriebs- und auch seine Cybersicherheit zu verbessern.“

Lars Bajlum Holmgaard Christensen, Chef des *Danish Hub for Cybersecurity*, kann sich noch gut daran erinnern, wie bei Unternehmen ein Bewusstsein für Sicherheitslücken entstand, nachdem die ersten Informationen darüber publik geworden waren. „Für viele Unternehmen“, meint er, „war das ein Weckruf. Das Bewusstsein für die Bedrohungen ist nach diesen Cyberangriffen gestiegen.“

Im CFCS wurde ein 24/7-Lagezentrum eingerichtet, das an der landesweiten Cyber-Lageerkennung mitwirkt. Darüber hinaus sind 25

konkrete Initiativen geplant, um die Verteidigungsmaßnahmen gegen Cyberattacken, IT-Kriminelle und externe Bedrohungen zu stärken.

Das Beispiel des NATO-Landes Dänemark hat gezeigt, wie fragil das technische Gleichgewicht geworden ist in einer Welt, in der Big Data – durch die Möglichkeiten der KI noch potenziert – ein neues Bewusstsein für digitale Schwachstellen eröffnet und die Angriffe durch Cyberkriminelle zunehmen.

Während „die russischen Hacker" von der westlichen digitalen Welt als Bedrohung wahrgenommen werden, bleibt die Haltung Moskaus gegenüber diesen Gruppen ambivalent. Einerseits streitet der Kreml kategorisch ab, dass offizielle russische Stellen in solche Angriffe involviert seien. Andererseits gibt es in den Behörden einen gewissen – von der offiziellen Propaganda unterstützten – Stolz auf das, wozu russische IT-Freaks mutmaßlich in der Lage sind.

Nach Meinung des russischen Internet-Experten Alexander Isavnin, der an der Freien Universität Moskau lehrt, „kann von einer besonderen Abneigung der ‚russischen Hacker' gegen Dänemark keine Rede sein". Diese Hacker würden vielmehr eine Reihe von Schwachstellen – oft auch in verschiedenen Ländern – ins Visier nehmen und einzeln angreifen, um mehrere „Sicherheitsschleusen" nacheinander zu durchbrechen. Die am weitesten verbreitete Internetprotokoll-Version 4 (IPv4) bietet – im Gegensatz zu ihrer Nachfolgerin IPv6 – dank der begrenzten Anzahl von IP-Adressen und der aktuellen Netzwerkgeschwindigkeiten die Möglichkeit, fast das gesamte Internet innerhalb von Minuten nach Schwachstellen zu durchsuchen.

Während „die russischen Hacker" von der westlichen digitalen Welt als Bedrohung wahrgenommen werden, bleibt die Haltung Moskaus gegenüber diesen Gruppen ambivalent.

Hinter solchen Angriffen können, wie Isavnin einräumt, ganz unterschiedliche Akteure stehen: militärische Forschungseinrichtungen, über verschiedene Tech-Plattformen agierende Outsourcer, Betreiber von in Auftragsarbeit entwickelten Schadprogrammen oder auch moderne IT-Einrichtungen, vergleichbar den sogenannten *Scharaschkas* – den Forschungslaboren im sowjetischen Straf- und Arbeitslagersystem der Gulags. Das operative Ziel dieser Akteure besteht meistens darin, nach geheimen und schwer zugänglichen Informationen zu fischen oder Chaos zu stiften. Dass diese Attacken bislang möglich sind, liegt daran, dass es an weltweit abgestimmten Verfahren für den Umgang mit Cyber-

Akteuren fehlt.

Bei all diesen Entwicklungen sollte ein wichtiger Faktor jedoch nicht übersehen werden, der sicherlich seinen Anteil daran hat, dass Dänemark in der Comparitech-Weltrangliste den ersten Rang belegt: Anders als die USA gilt Dänemark derzeit nicht als hochkarätiges Ziel für Cyberangriffe.

Obwohl das CFCS in seiner Lagebeurteilung vom Juni 2021 das Gefährdungsniveau in Bezug auf Cyberspionage und Cyberkriminalität als sehr hoch einschätzt, ist die Bedrohung durch zerstörerische Cyberangriffe auf dänische Behörden und Privatunternehmen nach wie vor gering. Die dänischen Geheimdienste halten es daher für wenig wahrscheinlich, dass in absehbarer Zeit eine ähnliche Attacke wie der gezielte Ransomware-Angriff auf die US-Pipeline Colonial auch in Dänemark passieren könnte.

Solange dies so bleibt, wird sich Dänemark sicherlich weiterhin im Bereich der Cybersicherheit engagieren und dabei auch Wege beschreiten, die dem Rest der Welt durchaus innovativ erscheinen. Im Rahmen seiner internationalen Bemühungen wird Dänemark seine „Cyberdiplomatie“ weiter ausbauen. Im Jahr 2017 wurde der erste „Techplomat“ der Welt berufen, der die Interessen des Landes im Silicon Valley stärker vertreten soll. Derzeitige Amtsinhaberin ist die Tech-Botschafterin Anne Marie Engtoft Larsen, die den „Pionier“ Casper Klynge abgelöst hat.

Ein weiteres Aktionsfeld mit wachsendem Potential ist die Verknüpfung verschiedener Cybersicherheitslösungen mit innovativem dänischen Design. Die Sicherheitslösungen können schon im Stadium der Produktskizze als Teil des Gesamtpakets angeboten werden. Während die Debatte um dieses neue Marktverständnis Fahrt aufnimmt, erkennt die dänische Wirtschaft in der Cybersicherheit mehr und mehr ein neues, vielversprechendes Wachstumsmodell.

Aus dem Englischen von Christine Hardung



Ekaterina Venkina

Ekaterina Venkina ist Nachrichtenredakteurin bei der Deutschen Welle in Bonn und berichtet über weltpolitische und regionale Themen aus Russland und der ehemaligen UdSSR. Venkina gehört dem journalistischen Netzwerk n-ost in Berlin an.