Der Handel mit Sicherheitslücken

➤ **Vergleich mit anderen Ländern:** Wenn die deutsche Behörde Zitis letztlich operativ werden sollte, wird sie in Konkurrenz zu vielen Institutionen weltweit stehen, die nach Verwundbarkeiten in jener Massentechnologie suchen, die Millionen von Menschen täglich benutzen. Die meisten anderen derartigen Einrichtungen sind allerdings privatwirtschaftlich organisiert und gewinnorientiert. Sie finanzieren sich durch den Verkauf gefundener Sicherheitslücken an Interessenten. „Das ist finanziell weitaus lukrativer, als die Sicherheitslücken etwa den IT-Herstellern zu melden, damit diese geschlossen werden. Wer die Käufer solcher Sicherheitslücken sind, wird nicht transparent", sagt IT-Experte Jürgen Neuschwander. Auch Staaten und Polizeibehörden und Geheimdienste kauften auf diesem Markt ein.

➤ **Verwendungsmöglichkeit:** Die Malware kann zur Verbrechensbekämpfung eingesetzt werden oder auch zur Entdeckung regimekritischer Gegner in Diktaturen. Da diese Sicherheitslücken allerdings ebenso im Darknet vertrieben werden, ist davon auszugehen, dass auch alle Arten von Kriminellen sich auf diese Art ihre effizienten Cyberwerkzeuge beschaffen.

➤ **Schattenmarkt:** Im Darknet (der größte Teil des Internets) entstand weltweit ein Schattenmarkt, in dem aggressiver Computercode gehandelt wird. Um welche Summen es dabei geht, kann man auf der Webseite des umstrittenen Händlers Zerodium nachlesen. Das Unternehmen will Hackern für bisher unbekannte Sicherheitslücken sowie Werkzeuge, um diese auszunutzen, bis zu 1,28 Millionen Euro zahlen. „Man kann davon ausgehen, dass die Motivation von Programmierern, Sicherheitslücken zu finden und an solche Institutionen zu verkaufen, eine ganz andere ist, als in staatlichen Behörden, wie dem ZITIS, wo Programmierer mit Gehältern des öffentlichen Dienstes für Ihre Ergebnisse entlohnt werden", so Neuschwander.

➤ **Spektakulärer Hacker-Angriff:** So wurde beim „Pegasus"-Angriff auf das iPhone eines Menschenrechtlers in den Vereinigten Arabischen Emiraten Anfang 2017 einer der bisher spektakulärsten Hacks des iPhones bekannt. Die Angreifer konnten drei Schwachstellen in Apples Systemen ausnutzen, indem zum Beispiel Skype-Gespräche mitgelesen, auf E-Mails zugegriffen oder Tastaturanschläge protokolliert werden konnten. (sap)

Hacken mit staatlicher Anordnung: Eine neue Sicherheitsbehörde soll Messenger knacken. BILD: DPA

Die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (Zitis) hat in München den Betrieb aufgenommen. BILD: DPA

Sache, beispielsweise zu sagen: Liebe Firma Apple, wir haben bei euch im Betriebssystem IOS eine Schwachstelle gefunden. Macht die mal zu. Aber genau das wird nicht gemacht, denn man kann diese Schwachstelle für die Onlinedurchsuchung nutzen. Bei dem Erpessungstrojaner Wannacry war es eben genauso: Die Geheimdienstbehörde NSA hatte die Windows-Schwachstelle für die eigene Arbeit zum Ausspähen gelagert. Von dort war sie dann entwendet und im Internet auf Wikileaks veröffentlicht worden. Cyberkriminelle hatten damit ungehinderten Zugriff und konnten sie für eigene Interessen nutzen.

Müssen sich die Bürger darauf einstellen, dass der Staat in Zukunft weniger Interesse daran hat, diese Handys und die Privatsphäre zu schützen, und mehr ein Interesse daran hat, sie ausspionieren zu können und deshalb die Sicherheitslücken offen lässt?
Persönlich sehe ich das so: Im derzeitigen Gesetz der Vorratsdatenspeicherung werden alle Bürger zu potenziell Verdächtigen. Ob die vielen Daten bei der Aufklärung von Straftaten wirklich helfen, wurde nie wirklich bewiesen. Ich glaube, dass dieses Gesetz mittelfristig keinen Bestand haben wird. Die Massenüberwachung passt nicht zu unserer freiheitlichen, demokratischen Grundordnung und verletzt die Autonomie des Bürgers.

In den USA oder China ist das anders.
Stimmt, in Teilen von China wird der Bürger bereits auf Schritt und Tritt überwacht. In den Straßen gibt es Kameras mit Gesichtserkennung. Da werden Leute, die bei Rot über die Ampel gehen, öffentlich angeprangert und es gibt Minus-Punkte. Eine furchtbare Vorstellung. Das macht ja auch etwas mit den Menschen, wenn sie wissen, sie werden beobachtet. Sie passen sich an und verhalten sich anders. Man kennt das aus DDR-Zeiten.

Noch herrscht bei der Behörde Zitis akuter Personalmangel, derzeit sollen es weniger als 20 Mitarbeiter sein – von 120, die es noch dieses Jahr eigentlich sein sollten. Bis 2022 sollen sogar 400 Stellen besetzt sein. Eigentlich ist das doch eine interessante Stellenbeschreibung: Hacken mit staatlicher Anordnung. Was macht die Stellen dennoch so unattraktiv?
Erstens gibt es solche Experten de facto fast nicht am deutschen Markt und zweitens besteht ein Problem in der Bezahlung. Wer sich mit Hacker-Attacken und der Abwehr hervorragend auskennt, der verdient unter Umständen in der Wirtschaft im Monat, was der Staat in einem Jahr zahlt. Damit ist die Personalsuche ein sehr ernstes Problem.

Wenn schon kein monetärer Aspekt die neuen Mitarbeiter locken kann, was dann?
Es wird argumentiert, es sei der Reiz des Verbotenen. Wie Sie schon sagen: Hacken mit staatlicher Anordnung. Für IT-Spezialisten sind in der Privatwirtschaft gesetzlich enge Grenzen gesetzt, was man bezüglich Überwachung und Abhören tun darf, bei Geheimdiensten und zuständigen Behörden werden hier fast keine Grenzen gesetzt. Das könnte ein Argument für interessierte Nerds sein, sich hier auszutoben.

Wie bewerten Sie die Behörde insgesamt?
Trotz aller Kritik an Zitis ist der Ansatz zur Gefahrenabwehr nicht falsch, bedarf aber einer strengen Kontrolle. Natürlich muss die Behörde noch beweisen, ob sie die an sie gestellten Anforderungen auch erfüllen kann. Organisationstheoretisch betrachtet ist die Idee vom Effizienzgedanken her richtig. Denn wenn 16 Landeskriminal- und Verfassungsschutzämter jeweils ihre eigene Software entwickeln und dazu Spezialisten brauchen, ist das sicher weder ressourcen- noch kostenoptimal.

FRAGEN: SANDRA PFANNER

---

pendeln. Früher wäre bei solchen Distanzen ein Umzug nötig gewesen. „Auf der anderen Seite senken technische Neuerungen nicht zwingend die Mobilität. Da heute Videokonferenzen kein Problem sind, könnte man erwarten, dass Arbeitnehmer dadurch weniger reisen – die Daten deuten jedoch darauf hin, dass dem nicht so ist", sagt Gerstenberg.

Problematisch sei diese Entwicklung deshalb, weil Mobilität die Gesundheit belaste: So klagen laut Gerstenberg Pendler überdurchschnittlich häufig über eine Beeinträchtigung ihres Wohlbefindens. Komme dann noch Schichtarbeit hinzu, steige das Risiko für Herzprobleme, Kopfschmerzen, Müdigkeit, Nervosität und Schlafprobleme signifikant. „Wichtig sind beim Pendeln auch die Kontextbedingungen – Pendeldauer und Entfernung, aber auch Vorhersehbarkeit, Beeinflussbarkeit und Planbarkeit", sagt Susanne Gerstenberg. Je weniger für die Beschäftigten kalkulierbar sei, wann sie Feierabend haben – etwa wegen eines Meetings oder einer Sonderaufgabe – desto stärker falle ihre Stressreaktion aus.

„Die Zeit, die für das Pendeln aufgewendet wird, hat in den vergangenen Jahren zugenommen."

Susanne Gerstenberg,
Bundesanstalt für Arbeitsschutz

Nicht nur die betroffenen Arbeitnehmer bekommen den Anstieg des Pendelns zu spüren – auch in der Umwelt zeigen sich Auswirkungen. „Der Flächenverbrauch und die Verkehrsbelastung steigen", sagt Harald Herrmann, Direktor des Bundesinstituts für Bau-, Stadt- und Raumforschung in Bonn, das diesen Aspekt untersucht hat. Denn die Zahl der Pendler ist den Angaben zufolge von 53 Prozent der Arbeitnehmer im Jahr 2000 auf 60 Prozent im Jahr 2015 gestiegen.

Hinzu kommt, dass auch die durchschnittliche Länge des einfachen Arbeitsweges zugenommen hat: von 14,6 Kilometern im Jahr 2000 auf 16,8 Kilometer im Jahr 2015. Durchschnittlich 45 Minuten ist ein Pendler unterwegs. „Deshalb ist es wichtig, dass die Infrastruktur mit dem Wachstum Schritt hält und das Umland gut an den öffentlichen Nahverkehr angebunden bleibt", sagt Herrmann.

Gerstenberg von der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin sieht auch die Arbeitgeber in der Pflicht. Für die Mitarbeiter und ihre Gesundheit sei es „wichtig, auf Kalkulierbarkeit hinzuwirken – etwa durch Gleitzeitregelungen, durch die Beschäftigte ihre Arbeit unabhängig von der Verkehrssituation gestalten können".

INTERAKTIV

CHROME

Erweiterung schöpft Facebook-Daten ab

Eine Chrome-Erweiterung namens Browse-Secure gibt vor, den Google-Browser sicherer zu machen. Tatsächlich schöpft sie aber Kontaktdaten aus den sozialen Netzwerken Facebook und Linkedin ab, wenn der Nutzer dort eingeloggt ist, warnt das Bundesamt für Sicherheit in der Informationstechnik (BSI). Betroffene Chrome-Nutzer sollten die inzwischen aus dem Chrome Webstore entfernte Erweiterung deinstallieren. Grundsätzlich gilt es, Browser-Erweiterungen vor der Installation genau so kritisch zu prüfen wie etwa Smartphone-Apps. (dpa)

HP

Neues Update schließt Sicherheitslücke

Rund 50 netzwerkfähige Druckermodelle von HP weisen eine Sicherheitslücke auf, über die Angreifer aus der Ferne auf die Geräte zugreifen und diese steuern können. Eine Liste mit den betroffenen Druckern hat der Hersteller bereits veröffentlicht. Nutzer sollten ein Firmware-Update installieren, das ebenfalls schon zur Verfügung steht, wie HP mitteilt. Auf der Seite www.hp.com unter „Support" und dann „Software & Treiber" kann über ein Suchfeld die Modellnummer eingegeben werden, wodurch man zum Download kommt. (dpa)

SERVICE

App erkennt langweilige Filmszenen im Kino

Viele Filmfans dürften schon einmal mit drückender Blase im Kinosessel gesessen haben. Die Angst, eine tolle Szene zu verpassen, ist eben mitunter stärker. Weiterhelfen will hier die App „RunPee.", für iOS und Android. Sie zeigt an, wann vergleichsweise uninteressante oder langweilige Szenen kommen – und wie lang diese sind, so dass man in dieser Zeit entspannt in Richtung Toilette verschwinden kann. Wer andere Kinobesucher nicht mit leuchtendem Smartphone-Display stören will, kann sich Pinkelpausen auch per Vibration signalisieren lassen.(dpa)

APPLE

Bluetooth und WLAN schneller abschalten

Mit iOS 11 als Betriebssystem lassen sich WLAN und Bluetooth nicht mehr über das Kontrollzentrum abschalten. Nutzer müssen zum kompletten Abschalten der Funkschnittstellen erst umständlich die Einstellungen aufrufen. Ein schnellerer Weg dahin führt über die 3D-Touch-Funktion, die es seit dem iPhone 6S gibt. Wer stärker auf das Einstellungen-Symbol auf dem Startbildschirm tippt, kann von hier direkt zu den entsprechenden Optionen springen und spart sich viel Tipperei. (dpa)

FOTOGRAFIE

Webseite hilft verpixelte Bilder aufzubessern

Viele ältere Fotos aus den früheren Jahren der digitalen Fotografie sind heute einfach nicht mehr gut genug. Vergrößerungen von Bildausschnitten sehen meistens nur krümelig aus. Die Webseite letsenhance.io (deutsch: „lass uns verbessern") will hier eine Lösung bieten. Wer Fotos hochlädt, übergibt sie einer künstlichen Intelligenz, die mit Hilfe von Maschinenlerntechniken das Bild analysiert und verbessert. Die Nutzung der Seite ist kostenlos. Allerdings ist das Anlegen eines Nutzerkontos dafür notwendig. (dpa)

Wer sein Kind zum Surfen an den Rechner lässt, sollte ihm Grenzen setzen. BILD: DPA

Den Computer für Kinder fit machen

Für manche Familien ist es ein leidiges Thema. Es geht um die Frage, wie lang und wie oft gespielt oder im Netz gestöbert werden darf. Natürlich gehen die Meinungen von Eltern und Kindern weit auseinander, wie viel genug oder zu viel ist. Windows und macOS bieten Eltern viele Möglichkeiten, Kindern bei der Benutzung von Computern zumindest technische Grenzen zu setzen. Die wichtigsten Antworten im Überblick:

➤ **Nutzerkonto:** Sowohl Windows 7 und Windows 10 als auch macOS erlauben in ihren Benutzereinstellungen das Einrichten von Nutzerkonten mit geringeren Zugriffsrechten. „Kinder bekommen keine Administratorenrechte, die bekommen nur Eltern", empfiehlt Peter Siering, von der Fachzeitschrift „c't". Mit einem solchen eingeschränkten Konto können Kinder nur mit Zustimmung der Eltern Programme installieren oder Einstellungen verändern.

➤ **Jugendschutz einrichten:** Apple macht es Nutzern hier leicht. Gleich bei der Einrichtung des Kontos können Nutzer die Kindersicherungsoption wählen. In einer Liste kann dann per Mausklick bestimmt werden, ob und wie lange Internet, iTunes und Spiele zur Verfügung stehen. Der Webcamzugriff lässt sich ebenfalls verhindern. Wer Windows 10 nutzt, hat mit Microsofts Familienfunktionen die Möglichkeit, mit seinem eigenen Konto verknüpfte Microsoftkonten für seine Kinder anzulegen. Auf diese Weise gewinnt man zahlreiche Möglichkeiten, die Computeraktivitäten des Kindes zu steuern – und bei Bedarf einzugreifen.

➤ **Zeitlimits:** „Ein Zeitlimit ist immer dann gut, wenn ein Kind von pausenloser Beschäftigung mit Medien überfordert ist", sagt Kristin Langer, Medientrainerin bei der Aktion „Schau hin! Was dein Kind mit Medien macht". Windows 7, 8, 10 und macOS erlauben das Anlegen von stundengenauen Zeiträumen, in denen ein Nutzerkonto Zugriff auf den Computer hat. So lassen sich Schlafenszeiten auch für einzelne Tage einstellen und durchsetzen, erklärt die Initiative „Klicksafe.de".

➤ **Filter einrichten:** Nicht alles im Web ist auch für Kinder geeignet. Hundertprozentigen Schutz vor unangemessenen Inhalten gibt es zwar nicht. Doch die Betriebssysteme bieten eine Filterung. MacOS etwa erlaubt Eltern, Listen von freigegebenen Webseiten anzulegen. Dann können Kinder nur diese Seiten ansteuern. Solche Ausschlusslisten (Blacklists) oder Freigabelisten (Whitelists) lassen sich in den Einstellungsmenüs vieler Router anlegen. Auch bestimmte Stichworte lassen sich sperren.

➤ **Nicht zu sehr überwachen:** Sowohl Microsofts Familienoptionen als auch die Kontenverwaltung von macOS erlauben Eltern einen ziemlich genauen Einblick, was ihre Kinder mit dem Computer machen: Etwa die Durchsicht besuchter Webseiten, Nutzungszeiten oder gestartete Programme. Medientrainerin Kristin Langer hält von so viel Kontrolle nichts: „Harte Kontrolle ist eine gute Basis für konfliktträchtige Auseinandersetzungen", sagt sie.

➤ **Im Gespräch bleiben:** Selbst die besten technischen Sperren können überwunden werden. Je älter Kinder werden, umso findiger werden sie bei der Umgehung von Sperren. Zu sehr sollte man sich darauf also nicht verlassen. Das Gespräch und vor allem das Verständnis für die Notwendigkeit mancher Regeln ersetzen sie nicht. „Manchmal sind solche Einstellungen gemein", räumt Kristin Langer ein. Statt Sperren einzurichten, plädiert sie dafür, Kindern immer zu erklären, warum sie für manche Inhalte vielleicht noch zu jung sind. Klare Verabredungen funktionierten häufig, so Langer. (dpa)