Thema vum Dag
Mehr zum heutigen Tagesthema „Cybersecurity Week“ finden Sie auf den folgenden Seiten
Seite 04 & 05

WO STEHEN WIR?

Teure Daten

Cybersicherheit betrifft jeden

Das wurde richtig teuer: British Airways erhielt nun einen Strafbescheid über 20 Millionen Pfund von der britischen Datenschutzbehörde wegen eines Diebstahls von Passagierdaten im Jahr 2018. Die Ermittler waren der Meinung, dass die Fluggesellschaft das Leck, durch das die persönlichen und finanziellen Daten von mehr als 400.000 Kunden entwendet wurden, frühzeitig erkennen und schließen hätte müssen. Am Montag beginnt in Trier ein Prozess der Superlative gegen vier Niederländer, drei Deutsche und einen Bulgaren, denen vorgeworfen wird, in einem alten Bundeswehrbunker bei Traban-Trarbach mehr als 400 Server, über die Kriminelle aus aller Welt Drogen oder Daten verkauften, Cyberangriffe starteten oder Falschgeld vertickten. Die größte Gefahr für Internetnutzer geht derzeit von Ransomware aus, wie aus dem rezenten Cybercrime-Lagebild des deutschen Bundeskriminalamts hervorgeht. Erpressersoftwares, die oft durch unbedachte Klicks auf manchmal täuschend echte E-Mails von renommierten Firmen auf Rechner gelangen, verschlüsseln die Daten darauf. Die Hintermänner verlangen dann Geld für Wiederentschlüsselung.

Die europäische Polizeibehörde Europol berichtet in ihrem rezenten „Internet Organised Crime Threat Assessment“ über zunehmende „Subscriber identity module swapping“-Betrugsfälle. Dabei geht es darum, volle Kontrolle über Telefonnummern zu bekommen. Die Täter durchforsten etwa gestohlene Datensätze oder einfach die sozialen Netzwerke nach Adressen, Bankverbindungen oder sonstigen persönlichen Informationen eines Handybesitzers und rufen dann bei deren Telefon-Providern an, bei denen sie etwa vorgeben, das Handy sei kaputt und eine Änderung der SIM-Karte beantragen. Haben sie Zugang dazu, ändern sie die Einstellungen so, dass sie volle Kontrolle über die Karte haben und über ein anderes Handy alle Daten des visierten Smartphone-Besitzers abgreifen können.

Bei einer rezenten Online-Pressekonferenz zur Vorstellung einer neuen Sensibilisierungskampagne von BEE SECURE berichtete die Leiterin des „Kanner a Jugendtelefon“, Barbara Gorges-Wagner, über zunehmende Anrufe von jungen Leute, aber auch Eltern, die weder aus noch ein wissen, weil sie selbst oder ihre Kinder mit freizügigen Fotos erpresst werden, die eigentlich nur für den Freundeskreis bestimmt waren. Die psychologische Belastung sei hoch. Betroffene könnten in Depressionen verfallen, oder sogar Selbstmordgedanken hegen. Sie erklärte auch, dass viele Jugendlich nicht wüssten, dass sie sich strafbar machen, wenn sie intime Bilder von minderjährigen Freunden und sogar von sich selbst versenden oder gar in die sozialen Netzwerke stellen...

Aus den genannten Beispielen wird wohl zur Genüge ersichtlich, dass die digitale Sphäre, die immer mehr unser Leben bestimmt und sicher auch zusehends erleichtert, auch eine Menge von Gefahren birgt.

Und auf die sollte man vorbereitet sein, ob als Unternehmen oder als Privatperson. In den nächsten Tagen gibt es auch in Luxemburg wieder eine „Cybersecurity Week“ im Rahmen des europäischen „Cybersecurity Month“, während der man sich wieder eine Unmenge von Informationen zu einem äußerst facettenreichen und deshalb komplexen Thema holen kann.

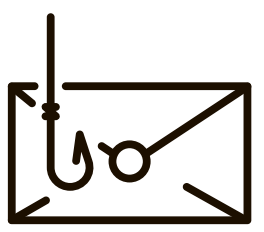
Doch bei aller Komplexität: auch im „Cyberspace“ gelten schon mal relativ einfache Grundregeln, um sich zu schützen. Dazu gehören etwa starke Passwörter, eine gute Portion Misstrauen gegenüber E-Mails von unbekannten Absendern, davon abzusehen, suspekte Datenanhänge zu öffnen oder auf komische Links zu klicken, alarmistische Meldungen von einer vermeintlichen Behörde, Bank oder Bekannten erstmal näher zu betrachten oder sich bei Problemen sofort an die zuständigen Stellen zu wenden - die man kennen sollte, wie man die Notrufnummer kennt. Alles Reflexe, die man trainieren muss. Haben Sie sie intus? Der Start der „Cybersecurity Week“ bietet auch Gelegenheit zum Selbsttest.

CLAUDE KARGER

EIN ANGRIFF ALLE 39 SEKUNDEN

Über **248** Milliarden US-Dollar werden 2023 für Cybersicherheit ausgegeben. 2017 waren es knapp **138** Milliarden

Alle **39** Sekunden passiert irgendwo eine Hackerattacke

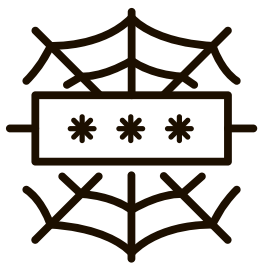


75 Prozent aller Cyberattacken beginnen mit einer E-Mail

67 Prozent der Datenlecks resultieren aus Identitätsklau, menschlichen Fehlern oder Druck auf Nutzer sozialer Netzwerke, Informationen preiszugeben

80 Prozent der Unternehmen beklagten während der Covid-19-Krise einen Anstieg der Cyberangriffe

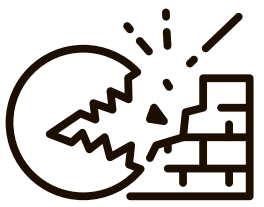
27 Prozent der Attacken nehmen Banken oder Gesundheitsdienste ins Visier



21 Prozent aller Online-Nutzer wurde schon Opfer von Hackern

Geschätzt **300** Milliarden Passwörter sind im Umlauf, die von Menschen und Maschinen genutzt werden

Die durchschnittliche Dauer zur Identifizierung eines Datenlecks lag 2019 bei **7** Monaten



3,92 Millionen Dollar Kosten verursacht im Durchschnitt ein Datenleck

133.000 Dollar Kosten für Unternehmen verursacht im Durchschnitt eine Ransomware-Attacke

Einige Zahlen zum Thema Cybersicherheit und Cyberkriminalität Quellen: Fintechnews, UK Web Host Review, andere

KLOERTEXT - EUGH-URTEEL ZUR VIRRATSDATESPÄICHERUNG

Lëtzebuerg nach ëmmer ontäteg

DENNIS FINK
Chaos Computer Club Lëtzebuerg

De 6ten Oktober huet den europäesche Geriichtshaff zu Lëtzebuerg, d'Virratsdatespäicherung nees eng Kéier als net konform zu den EU-Grondrechter deklaréiert. Den Dennis Fink vum Chaos Computer Club Lëtzebuerg erkläert, wéi dat kënnt:

„Nodeems den europäesche Geriichtshaff, d'Virratsdatespäicherung schonns 2014 gekippt huet, huet den deemolege Justizminister Felix Braz, gesot, si géifen d'Gesetz iwwerpréiwen. Ofgeschaaft ass et bis haut nach net! D'lëtzebuerger Regierung fuerdert léiwer d'Europäesch Kommissioun op, eng nei Direktiv ze erschafen. Dat mécht eis Regierung gäre bei netzpolitischen Themen, wann dréngenden Handlungsbedarf besteet!

Mir als Chaos Computer Club Lëtzebuerg sinn nach ëmmer der Meenung, dass eng Virratsdatespäicherung ouni konkrete Verdacht ee massiven Aschnëtt an d'Fräiheetsrechter vun de Bierger ass. Den EU-Geriichtshaff gëtt eis mat senger Decisioun och Recht. Och wa bei der Virratsdatespäicherung, de Contenu net mat gespäichert gëtt, si Metadaten awer mindestens genau esou detailléiert.

Als Beispill kann een hei Metadate vun engem Telefonat huelen. Hei géifen Telefonsnummeren, Dauer vum Telefonat, Datum an Auerzäit, an, grad bei Handyen, och Lokalisatiounsdonnée gespäichert ginn. Dëst erlaabt et zum Beispill, Beweegungsprofiller vun de Leit ze erschafen. Duerch Telefonsnummere kann een och ee sougenannte Social Graph erstellen. Beispillsweis loosse sech Partnerschaften oder aner Bezéiungen erausfannen. Niewebäi schaaft d'Virratsdatespäicherung eng stänneg Gefor vun Dateverloscht a Datemëssbrauch. Sie ënnergrueft de Schutz vu journalistesche Quellen a schwächt Pressefräiheet.

Mëttlerweil ginn et och scho Studien (https://tinyurl.com/c3lkloertext), déi beleeën, dass och ouni Virratsdatespäicherung eng effektiv Opklärung vun Strofdoten ka gemaach ginn.

Mir als Chaos Computer Club Lëtzebuerg fuerderen d'Regierung op, dass d'Virratsdatespäicherung endlech ofgeschaaft gëtt, an, dass keng Versich méi ënnerholl ginn, fir eng Virratsdatespäicherung ouni konkrete Verdacht anzeféieren. D'EU Kommissioun fuerderen mir dozou op, ee Verbuet zur genereller d'Virratsdatespäicherung ouni konkrete Verdacht auszeschaffen. Sou kann d'EU fräi vun enger invasiver Iwwerwaachung ginn.“

> „Eng Virratsdatespäicherung ouni konkrete Verdacht ass e massiven Aschnëtt an d'Fräiheetsrechter vun de Bierger“