Cybersicherheit geht uns alle an

23.10.2020
von

Beller, Tanja

Schlagworte

Cybersicherheit
Phishing
Digitalisierung
ECSM
Verbraucher
Künstliche Intelligenz

Es fühlte sich an wie ein digitaler Stresstest – Homeoffice, Homeschooling, Sport mit der Fitness-App, Musikunterricht der Kinder via Videoanruf. Die Liste lässt sich beliebig fortsetzen. Mit dem Lockdown sind die enormen Einsatzmöglichkeiten digitaler Anwendungen, aber auch die Abhängigkeiten und Risiken in der digitalen Welt besonders spürbar und alltäglich geworden.

Der Stresstest ist fürs Erste gelungen – die technischen Infrastrukturen haben funktioniert und es ermöglicht, einen Großteil des wirtschaftlichen und gesellschaftlichen Lebens nach Hause zu verlegen. Die IT-Verantwortlichen haben unter Hochdruck gearbeitet, um das notwendige Sicherheitsniveau zu halten. Denn das „Remote-Arbeiten“ bringt auch neue Gefahrenquellen mit sich. „The New Work: Digital und Sicher" stand daher im Mittelpunkt der virtuellen-Netzwerk-Veranstaltung der Allianz für Cyber-Sicherheit zur Eröffnung des diesjährigen European Cyber Security Month (ECSM). Dabei wurde deutlich, dass neben den technischen „Hard Facts“, die beispielsweise eine sichere Ausstattung und Verbindungen betreffen, keinesfalls die „Soft Skills“ und die Sensibilisierung der Mitarbeiter vernachlässigt werden dürfen. Bewusstsein, Awareness, für die neuen Gefahren zu schaffen, das ist eine wichtige Aufgabe – nicht nur für die Sicherheitsexperten.

Blog abonnieren

Bei der Veranstaltung wurde zum Beispiel berichtet, dass das persönliche Gespräch mit den Kollegen am Arbeitsplatz, der „Flurfunk" durchaus vor Cyberrisiken schützen kann. Etwa wenn eine Phishing-Mail im Gewand einer vermeintlichen betriebsinternen Anweisung zum Herunterladen eines Software-Updates daherkommt, könnte man am Kaffeeautomaten schnell einen Kollegen fragen, was es damit auf sich hat. Zu Hause würde man aber vermutlich schneller downloaden, ohne sich vorab rückzuversichern - selbst wenn einem die Mail verdächtig vorkommt.

*In unserem Blog lesen Sie mehr zum **Schutz vor Phishing**, wir haben auch eine **Broschüre zum Thema Phishing** eröffentlicht.*

Cyberkriminalität: Gefahr aus dem Netz steigt

Jede Organisation, jedes Unternehmen, jeder Staat – und jeder Bürger – ist ein potenzielles Ziel von Cybertätern. Und die Gefahr nimmt nicht ab, sie wächst: Das Bundeskriminalamt (BKA) stellt in seinem kürzlich vorgelegten **Lagebericht für 2019** hierzu fest, dass Cyberkriminalität im vergangenen Jahr um 15 Prozent zugenommen hat – Tendenz steigend. Cyberkriminelle arbeiten inzwischen hochprofessionalisiert, arbeitsteilig organisiert und global vernetzt. Wie schnell Cyberkriminelle in der Lage sind, aktuelle Entwicklungen in ihre Angriffsszenarien aufzunehmen, hat die Praxis nachdrücklich bewiesen: Schon kurz nach Ausbruch der Corona-Pandemie tauchten Phishing-Mails mit Corona-Bezügen in vielen Varianten auf. Gefälschte Behörden-Webseiten für Hilfsanträge oder sogenannte **Denial-of-Service-Angriffe (DoS)** mit dem Ziel, Webserver zu überlasten und dadurch den Zugriff auf die Website zu stören, sind weitere Beispiele. Schnell gab es auch Meldungen über Sicherheitsrisiken bei Anwendungen

für Videokonferenzen, die stark ansteigende Nutzerzahlen verzeichneten.

Höhere Rechner-Leistungen und neue Möglichkeiten von künstlicher Intelligenz (KI) helfen zwar bei der Gefahrenabwehr, werden aber vermehrt auch von den Kriminellen selbst eingesetzt. In Verbindung mit dem geschickten Ausnutzen menschlicher Eigenschaften wie Neugierde und Angst entsteht eine gefährliche Gemengelage. Es ist ein Nährboden für immer neue „Phishing-Narrative", also Informationen, Anhänge, Abfragen, die mittlerweile täuschend echt aussehen. Die Zeiten, in denen man gefälschte Webseiten oder Dokumente durch Rechtschreibfehler oder sprachlich ungeschickte Formulierungen schnell erkennen konnte, sind längst vorbei. Niemand sollte glauben, dass er davor gefeit ist, selbst auf Phishing-Angriffe hereinzufallen. Das BKA zieht aus seiner **Sonderauswertung Cybercrime in Corona-Zeiten** das Fazit, dass die Widerstandsfähigkeit der Bevölkerung und Unternehmen gegen unlautere Methoden von Social Engineering (also der Manipulation durch Kriminelle) weiter auf die Probe gestellt werde. Potenziell könne jeder betroffen sein.

Cybersicherheit: Grundregeln der „digitalen Hygiene" beachten

Händewaschen, Abstand halten, Maske tragen. Wir alle haben in der Pandemie erfahren, dass die Beachtung von Grundregeln der Hygiene vor Infektionen schützen kann. Es gibt auch Grundregeln einer „digitalen Hygiene" – quasi für das digitale Händewaschen zum Schutz vor einer viralen Infektion. Zu den Basisschutzmaßnahmen, die jeder Internetnutzer beherrschen und anwenden sollte gehören: Sicherheitsupdates und Antiviren-Software aktuell halten, nicht auf Links und Anhänge von unbekannten Absendern klicken, Datensparsamkeit beachten und sorgfältig mit sensiblen persönlichen Daten umgehen. Darüber hinaus ist die Aufklärung, Information und Sensibilisierung über die Cybergefahren eine Daueraufgabe im digitalen Raum. Zu Recht liegt deshalb der Fokus des europäischen Aktions-

monats zur Cybersicherheit in diesem Jahr auf den Themen digitale Kompetenz und Online-Betrug.

*Mehr zum Thema Online-Betrug können Sie in unserem **Lexikon zur Cyberkriminalität** nachlesen.*

Cyberrisiken sind für jede Wirtschaftsbranche relevant, für die Banken in besonderem Maße. Wir beim Bankenverband engagieren uns deshalb seit vielen Jahren mit umfassenden Informationen zur Prävention von Online-Betrug beizutragen. Auch in diesem Jahr beteiligen wir uns wieder am European Cyber Security Month (ECSM), dessen Organisatoren daran arbeiten, den Schutz vor Cyberkriminalität spürbar zu verbessern.