Cybersicherheit | 24.01.2019 | Nr. 032/19

Lukas Kilian: (TOP 25) Die Gefahr von Cyberattacken ist real

Es gilt das gesprochene Wort
Sperrfrist Redebeginn

Cybersicherheit ist ein wichtiges Thema. Die aktuelle Veröffentlichung der höchstpersönlichen Informationen von Politikern und Prominenten hat das Thema wieder auf die Tagesordnung einer breiten Öffentlichkeit gesetzt. Tatsächlich ist dieser Angriff jedoch nur ein Tropfen auf den heißen Stein. Tagtäglich tropft es Angriffe aus dem Netz. Dieser Tropfen landete nun aber mal wieder in den Nachrichtenzentralen, weil die Opfer bekannt sind.

Der Minister hat es eben sehr eindeutig aufgezeigt. Die Bedrohungslage ist enorm. Firmen, Arztpraxen, Kanzleien, durch hochprofessionelle Angriffe aus dem Netz, kann der unaufmerksame Klick auf einen Emailanhang oder das Öffnen einer unscheinbaren Word-Datei, ein absolutes Chaos auslösen.

Seit einigen Jahren beobachte ich auch als Rechtsanwalt eine drastische Zunahme von Cyberattacken bei mittelständischen Firmen und Handwerksbetrieben. Die Gefahr ist real.

Angriffsziele sind aber auch Universitäten, Krankenhäuser und Behörden. Der Minister hat es eben ausgeführt, wir sind mit Dataport als zentralem Dienstleister gut aufgestellt. Es gibt Vorsorgemaßnahmen und ein Notfallmanagement, wenn diese versagen. Das ist gut.

100% Sicherheit gibt es aber nicht. Wie immer kommt es auf die Anwendung an. Das gilt auch für private Nutzer, die im Internet zunächst erstmal eigenverantwortlich handeln.

Wer überall das gleiche Passwort benutzt und dies seit Einstieg ins Netz nie geändert hat, der handelt ungefähr so gewissenhaft, wie ein nicht angeschnallter Falschfahrer auf der Autobahn. Es kann gut gehen, die Wahrscheinlichkeit ist aber gering.

Sicherer ist es, dass Passwort regelmäßig zu ändern und dabei ein Passwort auszuwählen, dass eher so aussieht als ob man auf der Tastatur eingeschlafen wäre anstatt „Passwort1234“ oder „Schatzi“.

Das Problem bei Tagesordnungspunkten wie diesen ist, dass viele technische Fragen

Verantwortlich: Kai Pörksen | Düsternbrooker Weg 70, Landeshaus, 24105 Kiel
0431/988-1440 | info@cdu.ltsh.de | http://www.cdu.ltsh.de

unfassbar kompliziert klingen und man sich deswegen nicht unbedingt damit beschäftigt.

So klingt die 2-Faktor-Authentifizierung eher nach einem gewaltigen Aufwand für Sicherheitsnerds, als nach einer Lösung für Jedermann. Dabei nutzen wir alle schon seit Jahren beim Online-Banking genauso ein Verfahren. Gebraucht wird Passwort und eine TAN. Da wo es möglich ist, sollte 2-Faktor-Authentifizierungen genutzt werden.

Doch neben Sicherheitsmaßnahmen, die Nutzer treffen können, halte auch ich es für sinnvoll, auch die Internetwirtschaft in die Pflicht zu nehmen. Zum einen brauchen wir mehr Respekt vor dem Grundsatz der Datensparsamkeit. Für eine Online-Tischreservierung im Restaurant z.B. ist es mir unerklärlich, warum ich neben meiner Handynummer auch noch eine Emailadresse und ggf. noch weitere Daten preisgeben muss. Zum anderen muss die Online-Wirtschaft auch stets gehalten sein, ihre Systeme bestmöglich zu sichern. Ich begrüße daher die Initiative des Ministers, mit der Privatwirtschaft ins Gespräch zu kommen ausdrücklich und danke für den Bericht.

Verantwortlich: Kai Pörksen | Düsternbrooker Weg 70, Landeshaus, 24105 Kiel
0431/988-1440 | info@cdu.ltsh.de | http://www.cdu.ltsh.de