Quelle: Eisenhans – stock.adobe.com

Bedrohungen aus dem Internet (1)

IT-Sicherheitslage 2020

Wie in jedem Jahr wollen wir die IT-Sicherheitslage in Deutschland im vergangenen Jahr 2020 zusammenfassen und Ihnen auch Hilfestellungen geben. Was hat sich verändert und vor welchen Bedrohungen müssen Sie besonders auf der Hut sein?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Sicherheitsbehörde des Bundes (***https://www.bsi.bund.de/***). Zu den Aufgaben gehört z. B. die Abwehr von Hackerangriffen, Trojanern und Viren. Sicherheitsanforderungen für zukünftige 5G-Netze, Schutzmaßnahmen für das mobile Lernen, Home-Schooling, Corona-Warn-App, Strategien für die Regierung u.a. sind weitere Betätigungsfelder des BSI.

Folgen von Hackerangriffen

Die Folgen von Cyber-Angriffen sind abhängig vom Verhalten des Internetnutzers. Dabei ist ein Grundverhalten in der Gesellschaft zu beobachten, das Angreifer lockt. Hier einige Daten, die aus einer Umfrage von BSI-Fachgruppen zusammengetragen wurden. Demnach

- war jeder vierte deutsche Bundesbürger Opfer von Kriminalität im Internet
- benutzen ca. 60 % der Befragten ein Antivirenprogramm
- achten ca. 50 % auf sichere Kennwörter
- updaten ca. 25 % regelmäßige ihre Systeme automatisch
- nutzen gerade ein Drittel eine Zweifaktor-Authentisierung
- wissen ca. 50 % der Befragten über Sicherheitsmaßnahmen vor Cyber-Angriffen Bescheid und ca. 40 % setzen diese meistens auch um.

Überraschenderweise setzt aber nur ein Drittel der bereits attackierten Befragten die Sicherheitsmaßnahmen bei einem Problem um und nur ca. 25 % kennt die BSI-Webseite (**Bild 1**) BSI für Bürger (***www.bsi-fuer-buerger.de***). Jedoch ein Drittel der Befragten informiert sich hin und wieder über Internetsicherheit, aber ca. 25 % nie. Im Online-Banking liegt der Anteil bei 60 %, beim e-Shopping bei 40 % (der Befragten). Aus den Umfragen geht hervor, dass das Bewusstsein für IT-Sicherheit nicht in allen gesellschaftlichen Bereichen vorhanden ist. Die Aufklärung in Schulen, Bildungszentren und in Betrieben ist nach wie vor erforderlich.

Schadprogramme

Alle Computerprogramme, die ein System beschädigen oder Programme nachladen, gehören zu den Schadprogrammen. Vor allem über Anhänge, Links in E-Mails oder durch Erweiterungen von legitimen Programmen kann der Schadcode unbemerkt im Hintergrund auf das System gelangen. Schwachstellen in Soft-/ Hardware, in System-Schnittstellen oder das Verhalten des Mitarbeiters können dazu führen.

Es ist zu beobachten, dass innerhalb eines Jahres mal mehr oder weniger Schadcode-Varianten im Umlauf gebracht werden. Immer wieder kommt es zu starken Einbrüchen, wobei langfristig ein stetiger Anstieg deutlich wird. Die Gründe sieht AV-Test und BSI in der erfolgreichen Schutzwirkung von Windows. Das am häufigsten (mit 83% Anteil in Q1, 2020) verbreitete Betriebssystem ist auch bei Schadcode-Entwicklern sehr beliebt. Die Up-

Autor:
Claus Strobel, Dozent für IT/ET; Schwerpunkt Netzwerktechnik, etz Stuttgart

Bild 1: *Ansicht im Browser der Webseite www.bsi-fuer-buerger.de*

dates sorgen immer wieder für Einbrüche, weil sie die Systemlücken schließen und den Schadcode unbrauchbar machen. Der Angreifer wird nun herausgefordert, neuen Schadcode zu schreiben. Damit entstehen neue Varianten, die für den leichten Anstieg (Trendlinie) verantwortlich sind (**Bild 2**). Im Berichtszeitraum (von Juni 2019 bis Mai 2020; Quelle: AV-Test) wurden 117,4 Mio. Schadcodevarianten zusätzlich festgestellt. Das BKA verzeichnet ca. 312 000 neue Schadcodevarianten pro Tag (Cybercrime-Bundeslagebilder 2019). Im Folgenden werden wir einige Sonderformen kennenlernen und beurteilen.

Spam und Malware-Spam

Unerwünscht zugesandte E-Mails werden als Spam bezeichnet. Neben Werbe-E-Mails kann allerdings auch Schadcode durch E-Mails verbreitet werden. In diesem Fall spricht man von Malware-Spam.

Der Versand von unerwünschten Werbe-E-Mails ist gegenüber dem letzten Jahr weiter zurückgegangen. Das liegt an den verbesserten Spam-Filtern, die dafür sorgen, dass der E-Mail-Empfänger den meisten Spam gar nicht erst erhält. Spam und Malware-Spam sind nicht mehr lukrativ genug für den Angreifer.

Allerdings ist die Effektivität von Malware-Spam im letzten Jahr gestiegen, so das BSI in seinem jährlichen Bericht »Lage der IT-Sicherheit in Deutschland«. Das Verhalten von Internetteilnehmern wird über Webseiten, Online-Shops, Social-Media-Plattformen analysiert und gesammelt. Der Benutzer erhält Spam nach seinen Bedürfnissen. Das BKA brachte mit seinem jährlichen Report »Cybercrime Bundeslagebild« auf den Punkt: »***Jedes gestohlene Passwort, jede geleakte E-Mail-Adresse, jede erbeutete Kreditkartennummer kann für kriminelle Zwecke missbraucht und weiterverkauft werden.***«

Ein Ermittlungsverfahren wurde gegen einen 21-jährigen geführt, der unbefugt persönliche Daten und Dokumente von Politikern, Journalisten und Personen des öffentlichen Lebens veröffentlichte. Woher stammten diese Daten? Er bekam sie von dem Portal ***weleakinfo.com***, dass anschließend beschlagnahmt wurde. Das Portal erbeutete 12,4 Mrd. Datensätze aus über 10 000 aufgetretenen Datenlücken und bot ihm diese zum Verkauf an. Der Täter musste dort nur ein Taschengeld aufbringen, um an die Daten zu gelangen. Wer seine eigene E-Mail-Adresse überprüfen möchte, kann dies z.B. hier tun: ***https://haveibeenpwned.com***.

Im kommenden Teil wenden wir uns weiteren Schadprogrammen wie Botnetzen oder Ransomware zu.

(Fortsetzung folgt)

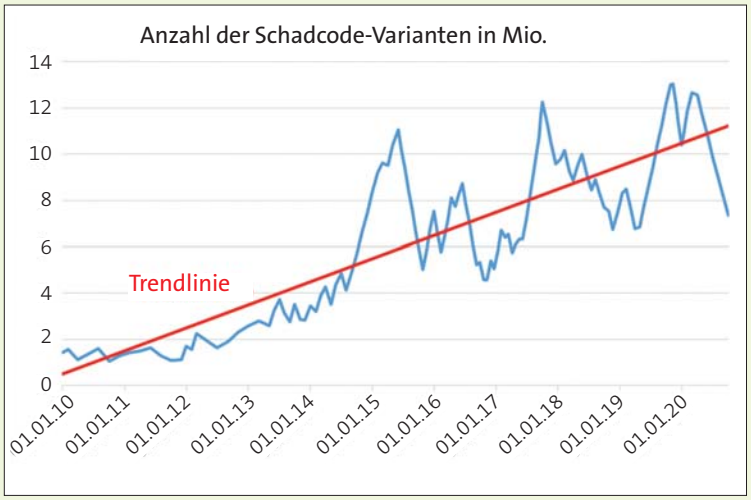

Bild 2: *AV-Test veröffentlich jährlich die IT-Sicherheitslage im Sicherheitsreport*

Quelle: beide Bilder C. Strobel