zvdh-kompakt

36/2019

Rund um Datenschutz und Cybersicherheit

Köln, 20. September 2019

Wir haben einige aktuelle Informationen des Bundesamts für Sicherheit in der Informationstechnik (BSI) zusammengetragen, um die IT-Sicherheit in den Betrieben zu erhöhen.

Software-Programme
Am 14. Januar 2020 endet der erweiterte Support für das Betriebssystem Windows 7 von Microsoft. Dies bedeutet für Anwender, dass sie ab diesem Zeitpunkt keine Sicherheitsupdates mehr erhalten und öffentlich bekannte Schwachstellen nicht mehr vom Hersteller geschlossen werden. Eine weitere Nutzung von Windows 7 birgt hohe Risiken für die IT-Sicherheit, insbesondere, wenn die betroffenen Systeme mit dem Internet verbunden sind. Mögliche Vorgehensweisen sind hier die Aktualisierung auf eine weiterhin unterstützte Version des Windows-Betriebssystems (Upgrade) oder der Wechsel zu einem alternativen Betriebssystem wie Mac OS oder Linux.
https://www.bsi.bund.de/dok/12713804

Ransomware: Bedrohungslage und Prävention
Ransomware sind Schadprogramme, die den Zugriff auf Daten und IT-Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (englisch: „ransom“) wieder freigeben. Besonders verbreitet sind Schadprogramme, die sich gegen Windows-Rechner richten. Prinzipiell aber können alle Systeme befallen werden – zum Beispiel Computer, die unter dem Desktop-Betriebssystem MacOS X laufen oder auch mobile Android-Geräte. Derzeit zielen die meisten Täter jedoch auf Windows-Systeme ab. In einer aktuellen Empfehlung hat das BSI zahlreiche Informationen zur Bedrohungslage in Sachen Erpressungstrojaner sowie Handlungsempfehlungen zusammengestellt:
https://www.bsi.bund.de/dok/7763952

Hoaxes (Falschmeldung)
„Hoax“ steht im Englischen für „schlechter Scherz“. Im Internet hat sich der Begriff als Bezeichnung für Falschmeldungen, vergleichbar mit Zeitungsenten, einbürgert. Darunter fallen falsche Warnungen vor bösartigen Computerprogrammen, die angeblich Festplatten löschen, Daten ausspionieren oder anderweitig Schaden auf den Rechnern der Betroffenen anrichten können. Hoaxes betreffen aber auch Petitionen gegen vermeintliche skandalöse Praktiken von Unternehmen („Verkauf von Bonsai-Katzen“), Aufrufe zu Knochenmarkspenden für nicht existente Personen oder „Geheimtipps“, um an schnelles Geld zu gelangen. Die meisten „Hoaxes“ enthalten folgende Elemente:

- Aufhänger, der Seriosität vermitteln soll (Bezug zu einem bedeutenden Unternehmen),
- angebliche Sachinformationen über ein Ereignis von besonderer Bedeutung (Auftauchen eines Computerschädlings), sensationelle Einkünfte (angebliche Provisionen durch Softwarekonzerne für die Weiterleitung von Mails), Hinweise auf Katastrophen (zum Beispiel Tsunami) oder Verschwörungstheorien,
- kein konkretes Datum, oft aber Bezüge wie „gestern“ oder „soeben“, um Dringlichkeit vorzutäuschen,
- dringender Aufruf, die Information oder Warnung möglichst schnell allen Bekannten zukommen zu lassen.

Gefälschte Absenderadresse
Spam-Mails haben fast immer eine gefälschte Absenderadresse. Ein Video des BSI erläutert, woran man gefälschte E-Mails erkennen kann:
Video E-Mail-Check

Herausgeber: Zentralverband des Deutschen Dachdeckerhandwerks e.V., Fritz-Reuter-Straße 1, 50968 Köln
☎ 0221-398038-0 0221-398038-99 E-Mail zvdh@dachdecker.de // Internet www.dachdecker.de
https://facebook.com/DachdeckerDeinBeruf Verantwortlich: Claudia Büttner