Bildquelle: Adobe Stock

Ist den Hackern der Einstieg ins System gelungen, nutzen sie die Daten gnadenlos aus.

Kampf den Hackern

Serie Digitalisierung, Teil 7: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat einige wichtige Informationen herausgebracht, die man kennen sollte, um die IT-Sicherheit im eigenen Betrieb zu erhöhen.

Claudia Büttner

Cyberangriffe mit der Schadsoftware Emotet haben in den vergangenen Tagen wieder erhebliche Schäden in der deutschen Wirtschaft, aber auch bei Behörden und Organisationen verursacht. Das BSI warnt daher erneut eindringlich vor dieser Schadsoftware und gibt ausführliche Hinweise zum Schutz vor Emotet. Auch Privatanwender stehen im Fokus der Angreifer, da Emotet weitere Schadsoftware nachlädt, die zu Angriffen auf das Onlinebanking genutzt werden kann.

„Viele dieser Schäden sind vermeidbar, wenn IT-Sicherheitsmaßnahmen konsequent umgesetzt werden! Dazu zählt unter anderem die Sensibilisierung der Belegschaft genauso wie regelmäßige Back-ups oder das Einspielen von Sicherheitsupdates", erklärt BSI-Präsident Arne Schönbohm. Die aktuellen Spammails zur Verbreitung von Emotet werden wie zuvor mit gefälschten Absendern als vermeintliche Antworten auf tatsächliche E-Mails versendet.

Sie enthalten entweder ein schädliches Office-Dokument (oft Word) direkt als Dateianhang oder einen Link, welcher zum Download eines solchen Dokuments führt. Über die in den Dokumenten enthaltenen Makros werden die Systeme mit dem Schadprogramm infiziert. Vor allem die in den Spammails enthaltenen Zitate aus einer vorhergehenden E-Mail-Kommunikation mit dem vermeintlichen Absender lassen die bösartigen Mails dabei für viele Empfänger authentisch erscheinen und verleiten sie zum Öffnen der schädlichen Office-Dokumente.

Softwareprogramme

Am 14.01.2020 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.
www.bsi.bund.de/dok/12713804

Bildquelle: Screenshot BSI-Webseite

Im Video auf der Website des BSI wird erklärt, woran man gefälschte Mails erkennen kann.

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 Lösegelds (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: *www.bsi.bund.de/dok/7763952*

Hoaxes (Falschmeldungen)

„Hoax" steht im Englischen für „schlechter Scherz". Im Internet hat sich der Begriff als Bezeichnung für Falschmeldungen, vergleichbar mit Zeitungsenten, eingebürgert. 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 vermeintlich skandalöse Praktiken von Unter-nehmen („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:

1. einen Aufhänger, der Seriosität vermitteln soll (Bezug zu einem bedeutenden Unternehmen),
2. 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,
3. kein konkretes Datum, oft aber Bezüge wie „gestern" oder „soeben", um Dringlichkeit vorzutäuschen,
4. dringender Aufruf, die Information oder Warnung möglichst schnell allen Bekannten zukommen zu lassen.

Gefälschte Absenderadresse

Spammails haben fast immer eine gefälschte Absenderadresse. Ein Video des BSI erläutert, woran man gefälschte E-Mails erkennen kann. Link aufs Video: *http://bit.ly/BSI-Mail-Check* //

Termine		
05.11.2019	2. Dach-Forum Mecklenburg-Vorpommern	Güstrow
16.01.–18.01.2020	Waldkirchener Meistertage	Waldkirchen
21.01.2020	Hamburger Dachtag	Hamburg
22.01.–24.01.2020	Mayener Meisterwoche	Mayen
28.01.–31.01.2020	DACH+HOLZ International	Stuttgart
26.03.–27.03.2020	Landesverbandstag Schleswig-Holstein	Bad Segeberg
08.05.–09.05.2020	Landesverbandstag Baden-Württemberg	Konstanz
03.07.–05.07.2020	Landesverbandstag Bayern	Bad Brückenau
Alle Termine der Branche finden Sie auf den Onlineplattformen www.ddh.de und www.dachdecker.de.		