6 Schadprogramme abwehren

ARGUMENTE:

Eines der Haupteinfallstore für Ransomware sind Makros, die sich in Dateianhängen von E-Mails verbergen. In vielen Fällen können sie eine Schadsoftware abwehren und einen Angriff mit Ransomware verhindern. Jeden Tag erscheinen hunderttausende neue Schadcodevarianten. Daher müssen die Software selbst und ihre Erkennungsdatenbank immer auf dem neuesten Stand gehalten werden.
Phishing per E-Mail ist ebenfalls ein zentraler Angriffsvektor. Insbesondere von gut gemachten Phishing-E-Mails lässt man sich leicht in die Irre führen.

FALLBEISPIEL

Die Mitarbeiterin eines Handelsunternehmens erhält eine gefälschte E-Mail eines vermeintlichen Kunden. Sie öffnet einen als Bestellung deklarierten Anhang, der Malware (Schadsoftware) enthält. Da Makros nicht deaktiviert sind, wird dadurch automatisch ein Verschlüsselungstrojaner installiert, der die Daten verschlüsselt.

FOLGEN

Der Geschäftsbetrieb ist nicht mehr möglich. Ein Backup ist auf einer externen Festplatte vorhanden, so dass der Datenverlust nur gering ist. Das System muss dennoch neu aufgesetzt werden.

WEITERFÜHRENDE INFORMATIONEN:

MAKROS DEAKTIVIEREN

Überlassen Sie die Entscheidung, ob ein Makro ausgeführt werden darf oder nicht keinesfalls den Beschäftigten – denn diese haben oft schlicht nicht die erforderlichen Kenntnisse, um so eine Entscheidung treffen zu können.

BSI – Cybersicherheit für KMU – Die TOP 14 Fragen, S. 14, Frage 5

https://sl.csc-kmu.de/b6-01.html

Konfiguration von Microsoft Access, Excel, PowerPoint, Word und Outlook.

BSI – Sichere Konfiguration von Microsoft Office 2013/2016/2019 v1.2

https://sl.csc-kmu.de/b6-02.html

VIRENSCHUTZPROGRAMME

Die im Handel erhältlichen (teilweise im Betriebssystem bereits enthaltenen) Virenschutzprogramme bieten automatische Updates und Speicherplatzüberprüfung. Diese Einstellungen müssen unbedingt aktiviert werden.

BSI – Cybersicherheit für KMU – Die TOP 14 Fragen, S. 15, Frage 6

https://sl.csc-kmu.de/b6-03.html

ABSICHERN VON VIDEOKONFERENZEN

Sind nur die autorisierten Personen Teil der Videokonferenz? Hinter einer ausgeschalteten Kamera kann auch ein Angreifer stecken, der mithören will. Die beliebten Screenshots von Videokonferenzen können wertvolle Informationen für Angriffe enthalten. Im Falle einer Veröffentlichung sollten sensible Daten wie URLs, Meeting-IDs sowie Namen und Gesichter unkenntlich gemacht werden.

CSBW-Factsheet zu Videokonferenzen

https://sl.csc-kmu.de/b6-04.html

!

NOTFALLKONTAKT CYBER-ERSTHILFE BW:

0711-137-99999