1 Wie funktioniert eigentlich ein „CyberAngriff“?

„Cyber-Angriffe“ erfolgen u.a. über die Einschleusung von Schadprogrammen (bspw. „Ransomware“ bzw. „Verschlüsselungs-Trojaner“). Damit versuchen Angreifer ihre Opfer durch Verschlüsselung des Datenbestandes arbeitsunfähig zu machen und im Anschluss Lösegeld für die Entschlüsselung der Daten zu erpressen.

2 Wie gelangt Schadsoftware in IT-Systeme?

Das Einschleusen von Schadprogrammen erfolgt bspw. über folgende Übertragungswege:

1. „Maliziöse E-Mail (-Anhänge)“

Öffnung schadhafter Datei-Anhänge (bspw. mit Datei-Endungen „.bat“, „.exe“)

2. „Schadhafte Internet-Downloads“

Öffnung schadhafter Datei-Downloads (bspw. mit Datei-Endungen „.bat“, „.exe“)

3. „Infektiöse Software-Updates“

Installation infektiöser Software-Updates (bspw. von korrumpierten Anbietern)

4. „Software-Schwachstellen“

Betrieb qualitativ minderwertiger Software-Systeme (bspw. von unseriösen Anbieter)

5. „Korrumpierte USB-Hardware“

Schleusung maliziöser Dateien (bspw. über korrumpierte USB-Hardware)

6. „Erbeutete Identitäten“

Angriffe mit erbeuteten Zugangsdaten (bspw. über „Phishing-Attacken“)

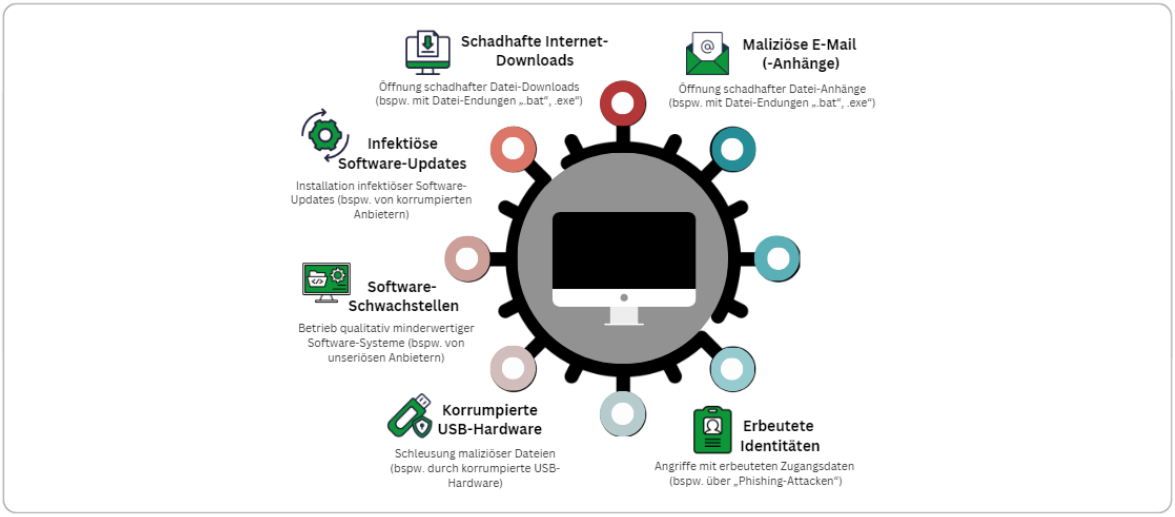

Abbildung 1: Übertragungswege von Schadprogrammen

Quelle: eigene Darstellung

3 Die Infektion eines IT-Systems in fünf Phasen

Die Infektion eines IT-Systems kann dabei folgendermaßen ablaufen:

1. Infektion

-Schadcode **erreicht** Opfer (bspw. „Dropper" via E-Mail)

-Schadcode wird **nachgeladen** (C&C-Server, Komplettierung)

2. Installation

-Schadcode **prüft** Zugriffs-Rechte (bspw. über Benutzer-Management)

-Schadcode **eskaliert** ggfs. Zugriffs-Rechte

-Schadcode **installiert** sich und wird Schadprogramm (bspw. „Ransomware")

3. Ausbreitung

-Schadprogramm **deaktiviert** Sicherungs-Systeme (bspw. Viren-Schutz)

-Schadprogramm **erbeutet** E-Mail-Adressen und **versendet** sich (bspw. via E-Mail)

4. Verschlüsselung

-Schadprogramm **verschlüsselt** Daten (bspw. auf lokalen Laufwerken)

-Schadprogramm **verschlüsselt** Daten (bspw. auf erreichbaren Speichermedien)

5. Geldforderung

-Lösegeldforderung zur Datei-Entschlüsselung **erreicht** Opfer

-Begleichung **ermöglicht** Entschlüsselung durch Kennwort

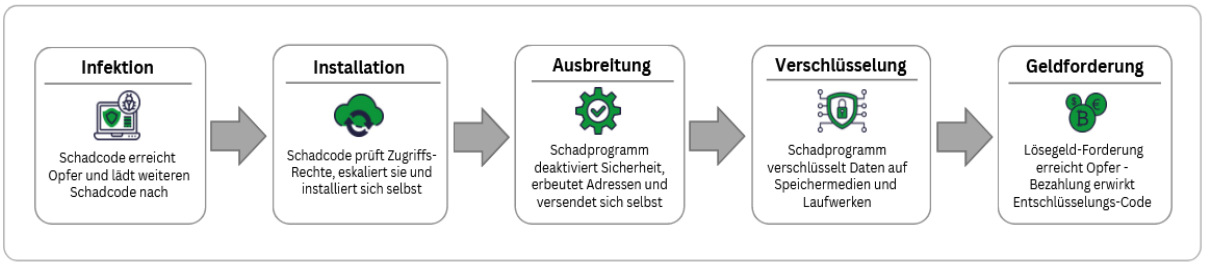

Abbildung 1: Übertragungswege von Schadprogrammen

Quelle: eigene Darstellung

4 Sieben Sicherheits-Maßnahmen zur Reduktion von Risiken

Folgende einfache Sicherheits-Maßnahmen reduzieren bereits wirksam die Risiken einer Infektion.

4.1 Viren- und Bedrohungsschutz aktivieren

Aktivieren Sie den Viren- und Bedrohungsschutz für alle Systeme. Darunter fallen Viren-Schutz, Firewall sowie ggs. auch App- und Browsersteuerung. Prüfen Sie diese regelmäßig auf Aktualität und Betriebsfähigkeit. Führen Sie regelmäßig vollständige Prüfungen ihres Systems durch. Dadurch wird Schadcode frühzeitig erkannt bevor Schaden entsteht.

4.2 System-Hygiene beachten

Halten Sie Software-Systeme stets aktuell, indem Sie „automatische Updates“ aktivieren und die automatische Ausführung von Software unterbinden. Prüfen Sie Einsatz-Notwendigkeit ihrer Software-Systeme und Seriosität der Anbieter und deinstallieren Sie unnötige Systeme. Dadurch werden Schwachstellen geschlossen und/oder Funktionen nachgerüstet bspw. um das Einschleusen von Schadcode zu verhindern.

4.3 Benutzer-Rechte einschränken

Richten Sie im Betriebs-System ein Benutzer-Konto mit reduzierten Rechten ein. Verwenden Sie dieses Konto für die tägliche Arbeit. Dadurch können Zugriffsrechte nicht eskaliert und Software nicht automatisiert installiert werden.

4.4 Identitäten stärken

Verwenden Sie starke Kennwörter und ggfs. Kennwort-Manager. Geben Sie niemals Ihre Identität (Login und Passwort) auf unbekannten Webseiten (bspw. „Phishing-Webseiten“) ein oder geben diese an Nicht-autorisierte Personen weiter. Dies verhindert den Diebstahl von Identitäten und verringert Ihr SPAM-Aufkommen.

4.5 Datei-Hygiene beachten

Ignorieren Sie SPAM-Nachrichten wie bspw. „Phishing-Attacken“. Achten Sie bei E-Mail-Anhängen und Internet-Downloads auf Datei-Endungen mit “.exe“, oder „.bat“ und zweifeln Sie diese grundsätzlich an.

4.6 USB-Hardware absichern

Inventarisieren und Kennzeichnen Sie Ihre USB-Geräte (bspw. USB-Speicher). Verleihen Sie diese nicht, formatieren Sie sie regelmäßig und vermeiden Sie das Schleusen unbekannter Dateien (bspw. von unbekannten Partnern).

4.7 Daten sichern

Sichern Sie Ihre Daten regelmäßig redundant, automatisiert bzw. manuell. Im Fall eines Angriffs können Sie diese wiederherstellen. Informieren Sie Ihre Partner im Notfall um diese ebenfalls zu schützen. So zeigen Sie Professionalität und sind zügig wieder arbeitsfähig. Üben Sie Notfall-Situationen durch Informations-Vorlagen, Wiederherstellen der Datensicherung und Prüfungen (bspw. durch Desinfektions-Software).

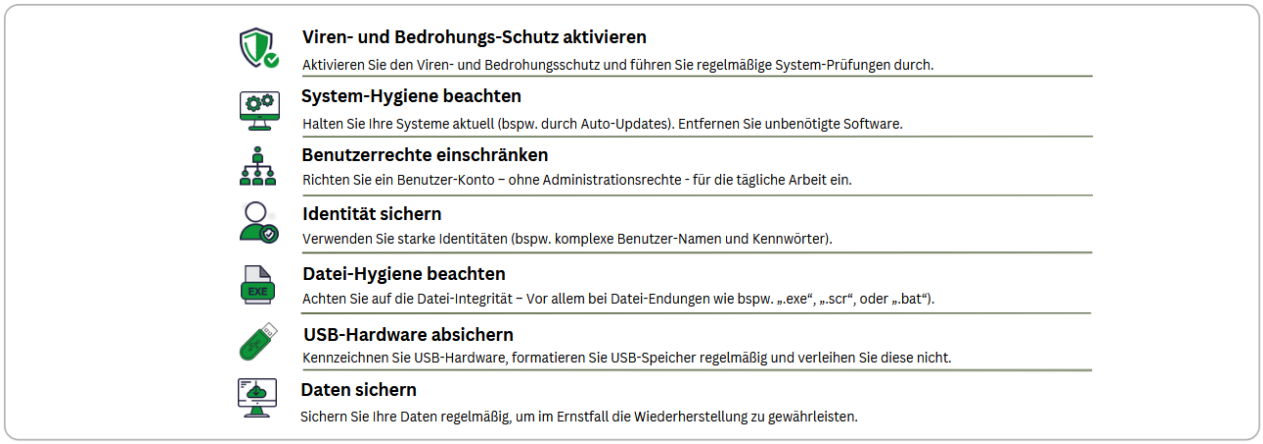

Abbildung 1: Übertragungswege von Schadprogrammen

Quelle: eigene Darstellung

5 Im Notfall: Notfall-Maßnahmen ergreifen

Ein CyberAngriff ist eine Straftat. Ziehen Sie Experten für IT-Sicherheit hinzu, um resultierende wirtschaftliche Risiken für Ihre Organisation zu vermeiden. Verständigen Sie ggfs. die Polizei.

Informieren Sie aktiv Ihre Geschäftspartner bspw. mit Hinweis auf der Website bzw. per E-Mail. Prüfen und bereinigen Sie Ihr System (bspw. mit Desinfektions-Software oder ggfs. Neu-Installation).

Kontakt:

www.digital-sicher.jetzt – eine Initiative der
Staatliche Lehr- und Versuchsanstalt für Gartenbau (LVG) Heidelberg
Diebsweg 2
D-69123 Heidelberg
Andy Höss
#bringdengartenbauinsicherheit

QR-Code für Download des

Infogrammes „CyberSicherheit - Maßnahmen zur Abwehr von Ransomware“