Bild: Fotolia-vchalup

Schutz vor digitalen Schädlingen

Risiken durch Viren, Würmer und Trojaner gezielt begrenzen

Digitale Gefahren wie Viren, Spionage- oder Erpressersoftware können SHK-Handwerksbetriebe nicht nur lahmlegen, sondern auch empfindliche Schäden verursachen. Schutzmaßnahmen gegen Cyberattacken sind deshalb unerlässlich. Doch welche Maßnahmen versprechen wirklich mehr Sicherheit?

Viele Handwerksbetriebe sind für Viren, Trojaner und Hacker ein leichtes Opfer: 80 % aller Betriebe hatten bereits mit IT-Sicherheitsproblemen zu kämpfen. Dies zeigt die Studie „Aktuelle Lage der IT-Sicherheit in KMU“, die das Wissenschaftliche Institut für Infrastruktur und Kommunikationsdienste (WIK) im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) zuletzt im Dezember 2017 durchführte und veröffentlichte. Ein wichtiger Grund für die Sicherheitslücken ist hier schnell ersichtlich: Nur 60 % der Handwerksbetriebe messen der eigenen IT-Sicherheit eine hohe Bedeutung

Ausgewählte Sicherheitslösungen im Überblick.

Hersteller	Avira	Bitdefender	Evorim	GData
Software	Antivirus (Pro)	GravityZone Business Security	Free Firewall	Antivirus
Funktionen	U.a. Virenschutz, Anti-Phishing und Webschutz	Sicherheitskomplettpaket, u.a. Virenschutz, Firewall, Anti-Phishing, Schutz vor Ransomware	Firewall zum Schutz vor Gefahren aus dem Internet	U.a. Virenscanner, E-Mail-Prüfung, Anti-Phishing, Anti-Ransomware
Betriebssysteme	Windows, Android, Mac, iOS	Windows, Linux, Mac, iOS	Windows, Linux, Mac	Windows, Mac
Preis (brutto)	Für Privat-Nutzer kostenlos. Business-Edition ab 34,51 Euro/Jahr pro Gerät (Rabattstaffel)	Ab 92,81 Euro/Jahr für drei Geräte/ ein Server	Kostenlos	29,95 Euro (Windows) bzw. 39,95 Euro (Mac)/Jahr pro Gerät (Rabattstaffel)
Internetadresse	www.avira.de	www.bitdefender.de	www.evorim.com	www.gdata.de

Tabelle: Stand 19. Juli 2019. Alle Angaben ohne Gewähr. Bilder: Hersteller

bei – und nur 39 % beschäftigen Mitarbeiter, die über IT-Sicherheitskenntnisse verfügen. Deshalb sind Cyberattacken auf Handwerksbetriebe immer wieder erfolgreich.

Dabei werden die Bedrohungen immer komplexer: Trojanische Pferde können zum Beispiel über eine Spyware-Funktion verfügen oder gleichzeitig Keylogger zum Auslesen von Passwörtern verwenden. Zudem nutzen einige Schadprogramme Update-Möglichkeiten, die neue Funktionen, Tarn-Mechanismen oder weitere Schadsoftware nachladen.

Eine akute Gefahr ist zum Beispiel der Trojaner „Emotet“: Dieser verbreitet sich über Spam-Mails und nutzt als Absender vertrauenswürdige Namen aus Kontaktlisten des Opfers. Öffnet der Empfänger infizierte Anhänge oder klickt auf Links im Mailtext, haben Hacker in kürzester Zeit die vollständige Kontrolle über das PC-System. Dabei wird unter anderem ein Banking-Trojaner auf dem Rechner installiert und eine Verschlüsselungssoftware nachgeladen. So wandelt sich Emotet zur Ransomware (Erpressersoftware): Der digitale Schädling verschlüsselt Inhalte von Festplatten, löscht gefundene Backups und verspricht Abhilfe ausschließlich bei Überweisung eines Lösegelds. Spätestens jetzt sind wertvolle Unternehmensdaten oft unwiederbringlich verloren – unabhängig davon, ob man die geforderte Summe zahlt oder nicht.

Checkliste: Schutz vor Schadsoftware auf allen Geräten

- Installieren und aktivieren Sie auf allen Geräten Firewall, Virenscanner und Phishing-Schutz.
- Halten Sie Betriebssysteme, Firewalls und Virenschutz per Updates immer auf dem neuesten Stand.
- Installieren Sie Spam-Filter und löschen Sie Spam-Mails ungelesen.
- Klicken Sie niemals auf Links in E-Mails, die Ihnen unaufgefordert zugesandt wurden.
- Öffnen Sie keine unbekannten Mail-Anhänge und starten Sie diese nicht – vor allem keine Office-Dokumente und Dateien mit Endungen wie „bat“, „com“ „exe“ oder „vbs“.
- Sperren Sie Datenlaufwerke, sofern Arbeitsabläufe nicht beeinträchtigt werden. So verhindern Sie das Einschleusen von Computerviren.
- Fertigen Sie regelmäßig Backups aller wichtiger Daten an und sorgen Sie dafür, dass Viren keine Sicherungskopien über das Netzwerk infizieren können.
- Sensibilisieren Sie alle Mitarbeiter für die Themen Datensicherheit und Datenschutz.
- Fragen Sie IT-Experten, Handwerkskammern oder Fachverbände, wie Sie die IT-Sicherheit in Ihrem Betrieb gezielt erhöhen können.

Mitarbeiter für IT-Sicherheit sensibilisieren

Eine Sensibilisierung der eigenen Mitarbeiter für die IT-Sicherheit des Betriebs ist deshalb besonders wichtig: Niemand sollte Anhänge von unbekannten Absendern öffnen oder auf verlinkte Inhalte in persönlichen Nachrichten klicken. Denn Schadprogramme gelangen nicht nur über verseuchte E-Mails oder Software auf eigene Geräte, manchmal genügt bereits das Aufrufen einer infizierten Internetseite. Bei aggressiven Viren, die tief in das Betriebssystem eingreifen oder ganze Netzwerke befallen, bleibt dann als Lösung oft nur das Formatieren aller Festplatten und das zeitaufwendige Neuaufsetzen aller Systeme.

Damit es so weit gar nicht erst kommt, können SHK-Handwerksbetriebe die Grundsicherheit der eigenen IT mit einfachen Schutzmaßnahmen deutlich verbessern. Ein guter Virenscanner, der sowohl E-Mails, Office-Dokumente, Programme, Apps und alle Internetaktivitäten überwacht, sollte zur Standard-

	Kaspersky	McAfee	Microsoft	Symantec	Zone Labs
	Small Office Security	Mobile Security	Windows Defender	Norton 360 Deluxe	ZoneAlarm Extreme Security
	Sicherheitskomplettpaket, u.a. mit Virenschutz, Anti-Spyware, Anti-Phishing, Verschlüsselung, Backup, Schutz vor Ransomware	Für Android: u.a. Virenschutz, Diebstahlschutz, Datenschutz, WLAN-Schutz Für iOS: u.a. Diebstahlschutz, Medientresor, Sicherheitsscan	U.a. Virenschutz, Firewall, Netzwerkschutz, E-Mail-Schutz, Webschutz	Sicherheitskomplettpaket, u.a. mit Firewall, Virenschutz, Anti-Spyware, E-Mail-Schutz, Passwortmanager	Sicherheitskomplettpaket, u.a. mit Firewall, Virenschutz, Anti-Spyware, Anti-Phishing
	Windows, Android, Mac, iOS	Android, iOS	Windows	Windows, Android, Mac, iOS	Windows, Android, iOS
	Ab 200 Euro/Jahr für bis zu fünf Workstations, fünf Mobilgeräte und ein Server	Kostenlos. Mehr Funktionen gegen Aufpreis	Bestandteil von Windows	34,99 Euro im ersten Jahr, danach 89,99 Euro/Jahr für bis zu fünf Geräte	26,95 Euro/Jahr pro Gerät (Rabattstaffel)
	www.kaspersky.de	www.mcafee.com	www.microsoft.de	www.symantec.de	www.zonealarm.de

ausstattung jedes Computers zählen. Nur so kann man sicher sein, dass nicht aus Versehen Viren, Würmer oder trojanische Pferde auf eigene Geräte gelangen, die Daten manipulieren, ausspähen und selbstständig verschicken. Gleichzeitig fahnden Virenscanner auch nach Spyware (Spion-Software), die sich meist unbemerkt installiert und dann Daten, Passwörter oder Verhaltensweisen des Nutzers ausspäht und per Internet versendet.

Virenschutzsoftware allein bietet aber keinen ausreichenden Schutz vor komplexen Bedrohungen: Ebenso wichtig ist eine Firewall, die Hacker-Angriffe abwehrt und gleichzeitig dafür sorgt, dass nur vertrauenswürdige Apps auf das Internet zugreifen können. Sonst besteht zum Beispiel die Gefahr, dass der eigene PC von Dritten ferngesteuert und für dubiose Hackertätigkeiten missbraucht wird – ohne, dass der Nutzer davon etwas mitbekommt. Zum eigenen Schutz gibt es sogenannte „Personal Firewalls", die einen einzelnen PC schützen, oder Gateway-Lösungen für ganze Netzwerke.

Checkliste: Maßnahmen nach Cyber-Attacken

1. Schalten Sie das betroffene Gerät sofort aus.
2. Trennen Sie Ihr Gerät von allen Netzwerken.
3. Ändern Sie mithilfe eines unbefallenen Geräts alle Passwörter für Dienste, die Sie auf dem infizierten Gerät genutzt haben.
4. Abhängig von Attacke und Schadenshöhe: Erstatten Sie Anzeige bei der Polizei. Klären Sie ab, welche Beweise zu sichern sind.
5. Falls möglich: Starten Sie das befallene Gerät mit einem bootfähigen Start-Medium (z. B. DVD oder USB-Stick).
6. Suchen Sie mit einem aktuellen Virenscanner auf dem befallenen Gerät nach Schadsoftware. So können Sie eventuell Daten retten, ohne die Schadsoftware zu verbreiten.
7. Ist eine Viren-Entfernung nicht möglich: Festplatten und Datenspeicher formatieren und das System komplett neu installieren. Gleiches gilt für befallene Netzwerk-Festplatten oder Server.
8. Je nach Schaden: Sperren Sie Ihre Kredit- oder Bankkarten.
9. Je nach Schaden: Prüfen Sie Ihre Melde- und Benachrichtigungspflichten laut DSGVO (Datenschutz-Grundverordnung).

Mobile Bedrohungen abwehren

Doch nicht nur Office-PCs und Notebooks sind von Cyberattacken bedroht – auch für Smartphones und Tablets sind Schadprogramme eine große Gefahr. Laut einer repräsentativen Umfrage im Auftrag des Digitalverbands Bitkom von November 2018 wurden 35 % aller Smartphone-Nutzer innerhalb der letzten zwölf Monate Opfer von bösartiger Software. Einen starken Anstieg von mobilen Gefahren zeigte auch im Oktober 2018 eine Analyse vom Cybersicherheitsunternehmen Kaspersky: Demnach sind Virenalarme auf Smartphones und Tablets in Deutschland innerhalb eines Jahres um 51 % gestiegen. Die Infektionen passieren meist bei der Installation scheinbar harmloser Apps, die Schadsoftware beinhalten und diese unbemerkt mitinstallieren. Deshalb sollten Virenscanner und Firewalls auch auf allen mobilen Geräten zur Grundausstattung zählen.

Wer sich für eine oder mehrere Sicherheitslösungen entscheidet, sollte allerdings einplanen, dass die Programme Systemressourcen verbrauchen und eigene Geräte deshalb etwas langsamer arbeiten – dafür aber sehr viel sicherer. Bei konkreten Fragen zum Thema IT-Sicherheit oder bei der Entwicklung eines IT-Sicherheitskonzepts für den eigenen Betrieb helfen die spezialisierten Berater der Handwerkskammern und Fachverbände weiter. ◀

Autor: Thomas Busch, Fachjournalist