Warnung

Am 02.03.2022 veröffentlichte die Stiftung Warentest das Ergebnis eines Vergleichstests von 29 Virenschutzprogrammen. Der Testsieger: Kaspersky. Zwei Wochen später wurden die Ergebnisse korrigiert: Zwar habe sich „an der Schutzwirkung der Kaspersky-Programme nichts geändert", dennoch sei „nicht auszuschließen, dass die russische Regierung Druck auf den Anbieter ausübt, um Änderungen an der Software zu erreichen, die sich negativ auf deren Funktionsweise auswirken". Da half auch die Versicherung des Herstellers wenig: „Wir gestatten Regierungsorganisationen niemals Zugriff auf Nutzerdaten oder unsere Infrastruktur – und wir haben niemals Aufforderungen erhalten, undeklarierte Funktionen in unsere Software einzubauen. Solche Aufforderungen werden grundsätzlich abgelehnt – und das wird auch in Zukunft so bleiben."

Am selben Tag (15.03.2022) veröffentlichte das BSI eine Warnung vor dem Einsatz von Kaspersky-Virenschutzprodukten – und löste damit in den IT-Abteilungen vieler Unternehmen und Behörden hektische Betriebsamkeit aus. Der Versuch von Kaspersky, rechtlich gegen die Warnungen der Bundesbehörde vorzugehen, scheiterte am 28.04.2022 vor dem Oberverwaltungsgericht Münster.

Was ist davon zu halten?

Natürlich stimmt das Argument, dass die hohen lokalen Berechtigungen eines Virenschutzprodukts, das zudem regelmäßig große Datenmengen (Signaturdateien) nachlädt, sich für einen nachrichtendienstlichen IT-Angriff oder eine Manipulation der Schutzwirkung geradezu anbieten. Nur: Kein Geheimdienst der Welt, der einen solchen Angriff plant, würde damit wochenlang warten – und vor „Cyberattacken" aus Russland hatte das BSI schließlich schon im Februar gewarnt.

Die Empfehlung, Kaspersky-Produkte zu ersetzen, greift daher viel zu kurz. Wer solche Angriffe befürchtet, sollte besser sofort seine gesamte Infrastruktur analysieren – denn wenn Angriffe geplant waren, muss man davon ausgehen, dass bereits Schadsoftware auf diesem Weg installiert wurde. Davon ist in der BSI-Warnung bedauerlicherweise nichts zu lesen.

Auch ist unverständlich, warum sich die BSI-Warnung auf Kaspersky-Produkte beschränkt. Alle relevanten Geheimdienste der Welt bauen seit Jahr(zehnt)en Cybercrime-Abteilungen auf. Mit ihren Attacken warten sie nicht auf einen begleitenden physischen Krieg – warum auch? Denn neben Russland sind auch China, Israel und die USA nicht nur technisch in der Lage, sondern auch gesetzlich autorisiert, solche Angriffe in „Friedenszeiten" durchzuführen, wie in der DuD 3/2022 Roßnagel, Geminn, Johannes und Müller ausführlich belegten.

Wer daher Kaspersky-Software verbannt, darf auch keine Checkpoint-Firewalls, Huawei-Smartphones, Lenovo-Laptops, Intel-Prozessoren und Cisco-Router einsetzen – und sollte besser auf die Nutzung von Microsoft-Programmen, Apple-Apps und Google-Diensten verzichten.

Nicht möglich, sagen Sie?

Richtig. Daher kommt es darauf an, bei der Angriffserkennung seine Hausaufgaben zu machen – damit man im Falle eines solchen Falles wenigstens zügig reagieren kann.

Dirk Fox