funkschau

business.technology.strategy

IfKom Ingenieure für Kommunikation

funkschau.de

Funkschau Leserwahl ITK-PRODUKTE DES JAHRES 2017

security Xpert

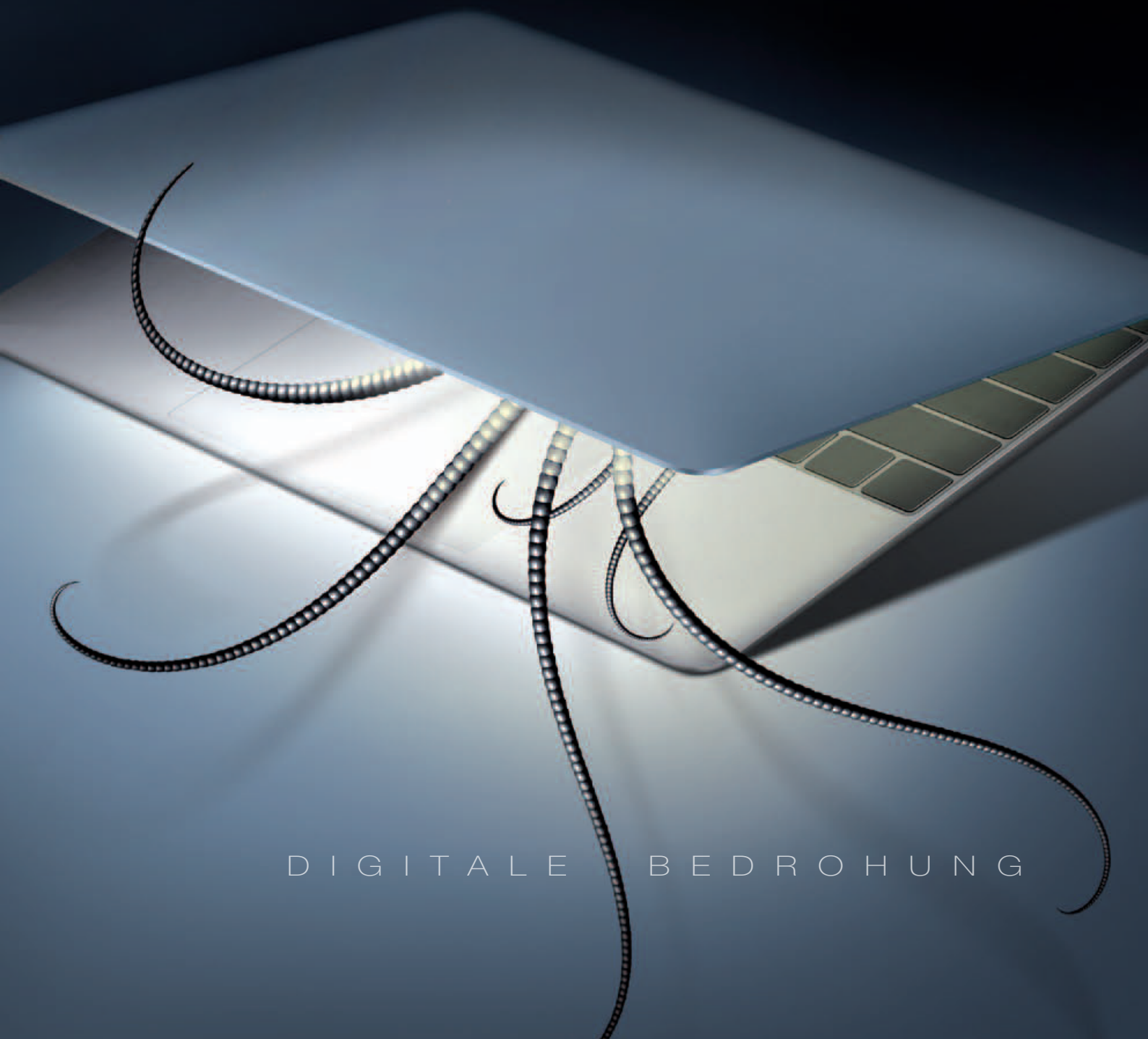
18

CYBERANGRIFFE IM WANDEL
Auslaufmodell Anti-malware-Lösung?

EU-DSGVO
Herausforderung Datenschutz

2017
29. September

€ 6,00 sfr 10,00



IST ANTIMALWARE-SCHUTZ NOCH NÜTZLICH?

Consecur hatte sich intensiv mit aktuellen Antimalware-Lösungen auseinandergesetzt, mit dem Ziel festzustellen, welche Erkennungsraten erzielt werden, wenn man die traditionelle signaturbasierte Erkennung eliminiert. Aufgrund der erhaltenen Ergebnisse hat die Unternehmensberatung für IT-Sicherheit sich stattdessen die Frage gestellt, ob Antimalware-Lösungen überhaupt noch nützlich sind.

Autoren: Stephan Ilic & Florian Krüp
Redaktion: Axel Pomper

➤ In guter Tradition verlassen sich auch moderne Antimalware-Lösungen auf signaturbasierte Erkennungsverfahren. Solche Signaturen werden durch die Analyse bisher unbekannter Malware erstellt, wobei eine Byte-Sequenz aus jener Malware entnommen und in einer Datenbank hinterlegt wird. Korrupt erscheinende Dateien werden dann mit den hinterlegten Sequenzen beziehungsweise Signaturen verglichen.

Eine weitere Möglichkeit Signaturen von Malware zu erzeugen ist die Anwendung eines Hashverfahrens. Hierbei wird die komplette Datei auf eine Zeichenkette bestimmter Länge abgebildet. Fortan fungiert dann diese Zeichenkette als Signatur. Problematisch bei dieser Methode ist, dass bereits eine leichte Modifikation der Malware zu einer anderen Signatur führen kann.

Eliminiert man nun die Möglichkeit von signaturbasierten Erkennungsverfahren, etwa bei Zero-Day Malware, kommt ein weiteres Erkennungsverfahren zum Tragen: die Heuristik.

Heuristische Verfahren

Nahezu jeder Hersteller von AV- oder Endpoint Protection-Lösungen benennt heuristische Verfahren als wirksamen Schutz gegen bisher unbekannte Malware. In diesem Zusammenhang bedeutet Heuristik, dass aus gegebenen Indikatoren geschätzt wird, ob es sich um schadhafte Software handeln könnte. Etwa, wenn die Software versucht Zugriff zu dem Betriebssystem-Kernel zu erhalten. Je mehr solcher für Malware charakteristischen Attribute gefunden werden, desto höher ist die Wahrscheinlichkeit, dass es sich um Malware handelt.

Consecur hat fünf verschiedene Lösungen mit acht unterschiedlichen Malware-Beispielen getestet und dabei festgestellt, dass keine Lösung alle acht Beispiele anhand der heuristischen Verfahren erkennen konnte, sondern maximal 50 Prozent erkannt wurden.

Die Ursache dafür liegt häufig tief im System selber: In der Softwareentwicklung ist es gängige Praxis ausführbare Dateien zu komprimieren, was dazu führt, dass Antimalware-Lösungen solche Dateien erst entpacken müssen, bevor sie untersucht werden können. Dieses Problem wird in der Regel auf zwei Arten gelöst: Für gängige Komprimierungsverfahren entwickeln Hersteller dedizierte Ent-

packer, die die Komprimierung rückgängig machen. Entwickler von Malware sind sich dessen bewusst und setzen vermehrt auf individuelle Komprimierungsverfahren, Hersteller wiederum auf Emulationen.

Beide Jobs, die Entwicklung von Entpackern und von Emulationsverfahren, sind aufgrund ihrer Komplexität schwierig umzusetzen. Rechnet man den Kosten- und Zeitdruck, welche auf der Herstellerseite allgegenwärtig sind, hinzu, ist es nicht weiter verwunderlich, dass das Konzept Security by Design in Sicherheitssoftware nicht in dem Maße berücksichtigt werden kann, wie man es wünschenswert wäre. Das Resultat dieser Umstände sind Antimalware-Lösungen, die zum einen Schwächen in Erkennungsverfahren aufweisen und zum anderen für eine gefühlte Sicherheit sorgen, während sie tatsächlich weitere Vektoren für Angreifer öffnen. Im Juni 2016 beschäftigte sich Google Project Zero mit Antimalware-Lösungen und fand teils erschreckende Schwachstellen in der Software von namhaften Herstellern.

Hinzu kommt, dass das Konzept der Endpoint Protection aufgrund der Funktionsweise andere Sicherheitskonzepte, wie zum Beispiel Ende-zu-Ende-Verschlüsselung, unter Umständen untergräbt. Bei der Endpoint Protection fungiert der Client als TLS-Proxy zwischen dem Browser und dem Webserver, um auch verschlüsselte Daten untersuchen zu können.

Vor wenigen Jahren konnten durch Antimalware-Lösungen noch etwa 70 bis 80 Prozent von Cybersicherheitsvorfällen aufgedeckt beziehungsweise verhindert werden. Seit dieser Zeit haben sich Methoden, Techniken und Taktiken von Angreifern massiv verändert, die Funktionsweisen von Antimalware-Lösungen jedoch kaum. In einer zunehmend digitalisierten Welt sind nicht mehr Computersysteme das erste Angriffsziel, sondern der Faktor Mensch, der aus Sicht des Angreifers mit wesentlich weniger Aufwand zu „hacken“ ist. An dieser Stelle hilft aber keine Sicherheitssoftware der Welt.

Rein funktional betrachtet sind Antimalware-Lösungen aber auch in der heutigen Zeit nicht nutzlos. Durch die Kombination von unterschiedlichen Erkennungsverfahren werden noch immer einige Cyber-Sicherheitsvorfälle verhindert, wenn auch zu einem wesentlich geringeren Anteil. Wodurch durchaus die Frage nach dem Verhältnis von Kosten zu Nutzen aufgeworfen wird.

Womit wir wieder bei der Frage sind: Sind Antimalware-Lösungen noch nützlich und zeitgemäß? „Jain“. Wobei die Antwort hier eher bei der Infrastruktur- und der vorhandenen IT-Security-Umgebung zu suchen ist. Neuere Sicherheitsansätze, wie etwa Security Information and Eventmanagement, beschäftigen sich nicht mehr mit dem Verhindern von Sicherheitslücken und dem schließen bekannter Sicherheitslücken. Viel mehr versuchen sie, aus oben beschriebenen Gründen, unbekannte Risiken, Sicherheitsvorfälle und Sicherheitslücken aufzudecken und Gegenmaßnahmen einzuleiten. Vor diesem Hintergrund gibt es durchaus Umgebungen, in denen Antimalware-Lösungen an Relevanz verlieren, doch totsagen sollte man diese dennoch nicht.

Stephan Ilic ist Senior Berater (SIEM) bei Consecur

Florian Krüp ist Junior Berater bei Consecur