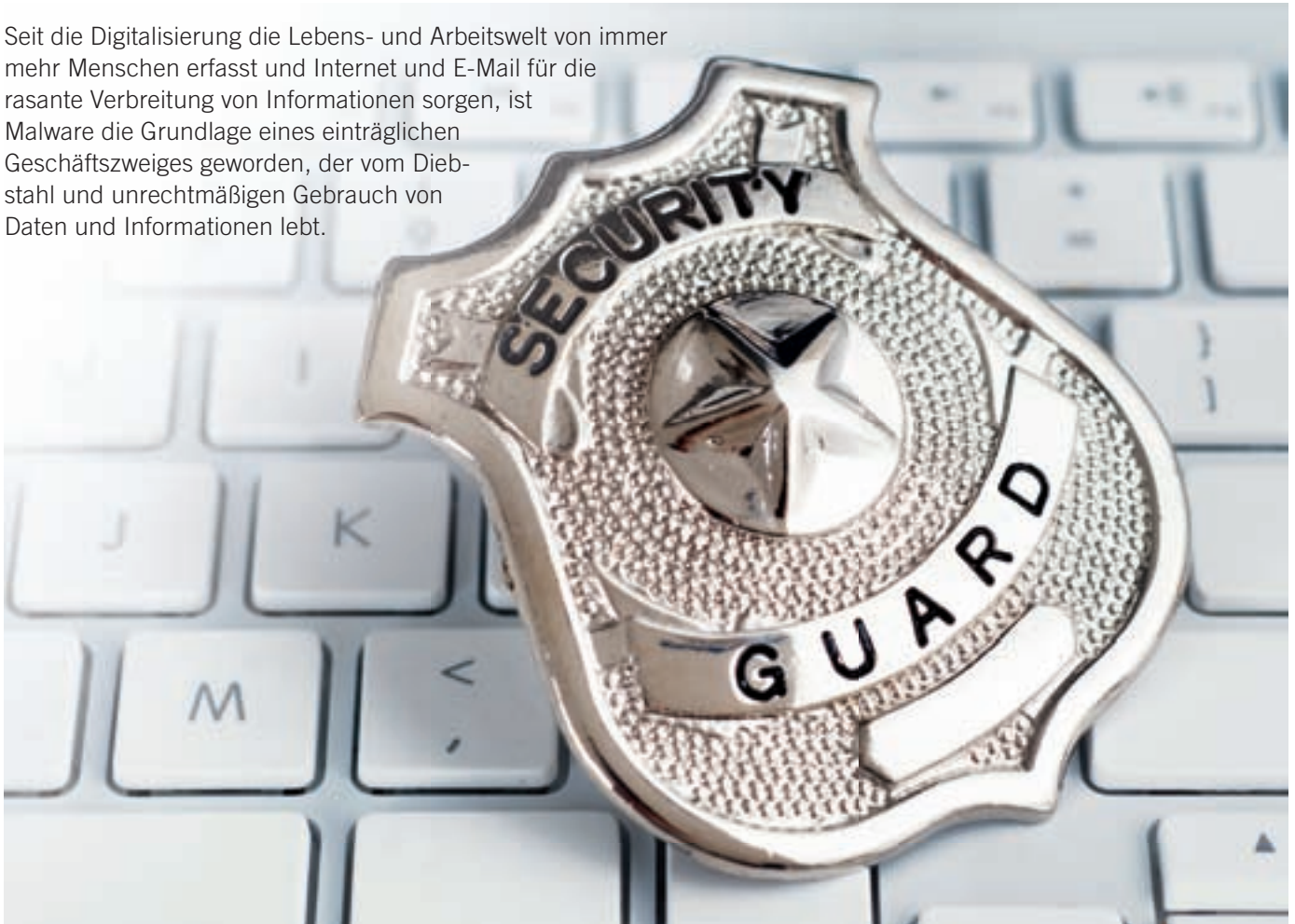


# Malware-Schutz in Bestform

Seit die Digitalisierung die Lebens- und Arbeitswelt von immer mehr Menschen erfasst und Internet und E-Mail für die rasante Verbreitung von Informationen sorgen, ist Malware die Grundlage eines einträglichen Geschäftszweiges geworden, der vom Diebstahl und unrechtmäßigen Gebrauch von Daten und Informationen lebt.



**M**it dem Auftauchen der ersten Computerviren 1988 in Norwegen spezialisierte sich das Unternehmen Norman auf Antivirenlösungen und hat im Lauf der Jahre ein breit gefächertes Spektrum an Technologien und Produkten zum Schutz von Unternehmensdaten entwickelt. Im Mittelpunkt des Schutzes der Unternehmensdaten steht der Arbeitsplatz-PC: Mit Kommunikationsschnittstellen aller Art bietet er Angriffsflächen, die von den Schutzeinrichtungen an den zentralen Zugangspunkten ins Unternehmensnetz nicht mit abgedeckt werden können. Lösungen direkt am Endpoint sollen deshalb verhindern, dass sich Gefährdungen von dort aus im gesamten Unternehmensnetz ausbreiten.

Zur Grundausstattung eines PCs gehört deshalb die Virenschutzlösung. Hohe Genauigkeit und Zuverlässigkeit machen sie unver-

## INFO

Norman zählt zu den führenden Unternehmen und Pionieren für die Entwicklung proaktiver Lösungen zur Absicherung von Unternehmensdaten und für die Entwicklung von Forensik-Tools zur Malware-Erkennung. Die Produkte von Norman schützen Endanwender und Netzwerke in Unternehmen jeder Größenordnung vor Malware und ermöglichen die Analyse von Schadcode. Norman wurde im Jahr 1984 in Oslo gegründet und vertreibt die Produkte weltweit über eigene Niederlassungen und ein ausgedehntes Partnernetz.

zichtbar. Sie schützt allerdings nur gegen Malware, deren Signatur in der Datenbank hinterlegt ist, neue Malware kann sie nicht identifizieren. Davon abgesehen braucht die Erstellung einer neuen Signatur Zeit. Bis sie auf den Anwender-Systemen angekommen ist, vergehen unter Umständen Stunden, in denen die Rechner ungeschützt sind.

Mit der Entwicklung der SandBox, die auf der Virus Bulletin International Conference 2010 als „innovativstes Konzept der vergangenen zehn Jahre“ ausgezeichnet wurde und in allen Virenschutzprodukten von Norman eingesetzt wird, hat Norman einen wichtigen Vorsprung im Kampf gegen Malware erarbeitet. Die proaktive Technologie kann Schadsoftware an ihrem Verhalten erkennen und schließt so die Lücke zwischen dem Auftreten neuer Malware und der Verfügbarkeit einer

## INTERVIEW

**FACTS: Immer mehr Hersteller im Bereich IT-Sicherheit bieten inzwischen Patch-Management-Lösungen an. Welchen Stellenwert haben Patches für die Endpoint-Sicherheit?**

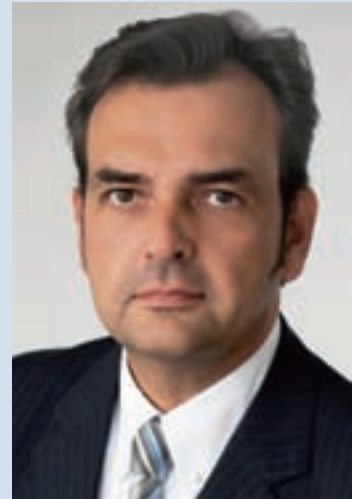
**Stefan Angerer:** Im Schnitt werden jeden Tag ungefähr 25 neue Schwachstellen bekannt; mehr als 90 Prozent der Angriffe nutzen Sicherheitslücken aus, die bereits bekannt sind und für die meist auch schon ein Update zur Verfügung steht. Patchen ist deshalb inzwischen so wichtig wie das tägliche Update der Virenschutzlösung, allerdings erheblich aufwendiger. Woran liegt das? Je größer ein Unternehmen ist, desto heterogener ist in der Regel die Client-Infrastruktur. Da gibt es nicht nur unterschiedliche Hardware-Typen und Hardware von verschiedenen Herstellern, sondern auch unterschiedliche Betriebssysteme sowie eine Fülle an Software. Aufgrund der unterschiedlichen Konfiguration der Clients müssen die Patches gewissermaßen individuell zusammengestellt und verteilt werden. Dass meist auch Third-Party-Produkte mitgepatcht werden müssen, auf die inzwischen mehr als 60 Prozent des Patch-Aufkommens entfallen, macht die Sache nicht einfacher.

**FACTS: Welches sind denn die entscheidenden Aspekte beim Patchen?**

**Angerer:** Beim Patchen stehen drei Aspekte im Vordergrund: Kritische Patches müssen zeitnah verteilt werden, und zwar auf täglicher Basis. Außerdem muss sichergestellt sein, dass die Patches nicht nur installiert werden, sondern auch installiert bleiben und nicht etwa durch Drittanbieter-Software überschrieben werden. Die entsprechende Prüfung sollte täglich erfolgen. Wichtig ist außerdem, dass Patches für Third-Party-Produkte mit dem gleichen Stellenwert wie Microsoft-Patches behandelt werden.

**FACTS: Was kennzeichnet eine zuverlässige Patch-Management-Lösung?**

**Angerer:** Eine Patch-Management-Lösung sollte drei Anforderungen erfüllen: Die Lösung sollte mit einer aktiven Komponente auf den Clients arbeiten. Nur so lässt sich überwachen, ob die Installation der Patches erfolgreich war, und sicherstellen, dass die Patches dauerhaft installiert bleiben. Eine weitere Anforderung ist die Herstellerunabhängigkeit der Lösung. Sie gewährleistet, dass Patches



Stefan Angerer, Geschäftsführer bei der Norman Data Defense Systems GmbH

für Third-Party-Produkte keinen zusätzlichen Aufwand machen und ebenso anstandslos wie die für Microsoft-Produkte verteilt werden. Außerdem sollten sinnvolle Tools für ein detailliertes Reporting verfügbar sein.

passenden Signatur. Ebenfalls auf Grundlage der SandBox gleicht Norman DNA Matching Instruktionen von unbekanntem Dateien mit den Code-Profilen bekannter Malware-Familien ab und erkennt damit neue Varianten. Als aktuelles Resultat von Normans Tradition im Bereich der Software-Analyse untersucht Norman Exploit Detection Dateien im Hinblick auf ihre Befähigung, Schwachstellen in Softwareprodukten für Angriffe zu nutzen. Innerhalb des Unternehmensnetzes schützt Norman Network Protection besonders sensible Netzwerkbereiche oder Anwendungen,

die nicht mit lokalem Malware-Schutz ausgestattet werden können.

### DATENVERLUSTE UNTERBINDEN

Ausgehend vom klassischen Virenschutz hat Norman das Portfolio um weitere am Endpoint wirksame Lösungen ergänzt: Norman Email Protection blockiert Spam, Malware und Phishing-Attacken bereits vor dem Eindringen in das Unternehmensnetz und filtert E-Mail-Anhänge auf unerwünschte Dateiformate. Optional werden Betreff, Body und Anhänge ausgehender E-Mails inhaltlich geprüft, sodass sich Datenverluste über diesen Kanal unterbinden lassen. Datenverluste über mobile Datenspeicher wie USB-Sticks beugt die Lösung Norman Device Control vor, indem sie den Datentransfer zwischen Datenspeicher und Endpoint überwacht und gegebenenfalls blockiert sowie Daten beim Überspielen verschlüsselt. Gleichzeitig wird die Gefahr verringert,

dass über mobile Geräte Malware ins Unternehmensnetz eingebracht wird.

Malware-Schutz unabhängig von Signatur-Updates leistet Norman Application Control. Mithilfe einer Whitelisting-Strategie wird sichergestellt, dass weder Malware aller Art noch unerwünschte beziehungsweise nicht lizenzierte Software am Arbeitsplatz-PC ausgeführt werden. Bei den zugelassenen Anwendungen stellt Norman Patch and Remediation einen optimal gepflegten Zustand sicher. Die Patch-Management-Lösung unterstützt die Systemadministration bei der Identifizierung von Sicherheitslücken im Unternehmensnetz und automatisiert und rationalisiert die Erfassung, Analyse und Verteilung von Patches.

Der Schutz der Unternehmensdaten kann aufgrund der Vielzahl und Beschaffenheit der Angriffsflächen am Endpoint heute nicht mehr von einer einzigen Lösung gewährleistet werden. Norman antwortet auf die Entwicklungen im Malware-Geschehen mit einem breit gefächerten Portfolio an Schutzlösungen, die an unterschiedlichen Angriffsflächen ansetzen und sich mit überlappenden Funktionen zu einem starken Schutzschild verstärken. (kl) ■

