# WIE EIN HACKER DENKEN

Solange es Wirtschaftsunternehmen mit Gewinnabsichten gibt, wird es Kriminelle geben, die sie bestehlen wollen und dazu alle Mittel, Wege und Schwachstellen nutzen. Im Kampf gegen solche Schurken müssen Sie selbst wie ein Hacker denken lernen. **Nur so erkennen Sie, welchen Gefahren Ihre eigenen Systeme ausgesetzt sind.**

## 6 SCHWACHSTELLEN, DIE HACKERGERNE NUTZEN

### 1 DIEBSTAHL UND VERLUST VON ENDGERÄTEN

GEFAHR

Diebstahl vertraulicher Daten

**80 %** **der Kosten** eines Laptop-Diebstahls entfallen **auf die gestohlenen Daten**[1]

LÖSUNG

Verschlüsseln Sie Endgeräte und setzen Sie ein Tool zur Verfolgung des Gerätebestands ein.

### 2 ARGLOSE ANWENDER

GEFAHR

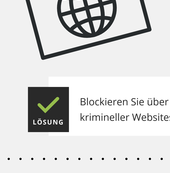
Schwache Kennwörter und Phishing-Angriffe

**85 %** **der Unternehmen** sind bereits Phishing-Angriffen zum Opfer gefallen[2]

LÖSUNG

Sensibilisieren Sie Anwender für mögliche Gefahren.

### 3 VERALTETER VIRENSCHUTZ



GEFAHR

Täglich gibt es neue Malware

**390.000** neue Arten von Malware **täglich**[3]

LÖSUNG

Sorgen Sie für aktuelle Virendefinitionen und nutzen Sie verhaltensbasierte und heuristische Analysen.

### 4 SOFTWARE OHNE SICHERHEITSPATCHES

GEFAHR

Veraltete Software ist anfällig für automatisierte Angriffe

**NUR 25 %** der Nutzer von Microsoft® Windows® haben ein aktuelles und vollständig gepatchtes System[4]

LÖSUNG

Ein Patch-Management-Tool hält alle Systeme auf dem neuesten Stand.

### 5 KRIMINELLE WEBSITES



GEFAHR

Drive-by-Downloads oder Kennwortdiebstahl durch Phishing-Sites

**195.000** Domains wurden für **Phishing-Angriffe eingesetzt** 2016[5]

LÖSUNG

Blockieren Sie über Webfilterung den Aufruf krimineller Websites.

### 6 FEHLENDE ÜBERWACHUNG



GEFAHR

Angriffe bleiben oft unerkannt

**205 TAGE** **dauert es im Schnitt,** bis ein Netzwerk-einbruch entdeckt wird[6]

LÖSUNG

Ein gutes Überwachungssystem erkennt Zugriffsversuche Unbefugter.

## SYSTEMEINBRÜCHE SIND TEUER. SENKEN SIE DAS RISIKO MIT SOLARWINDS® MSP

Holen Sie sich die Tools, die Sie für die Verwaltung, Absicherung und Optimierung der gesamten IT-Umgebung benötigen – innerhalb eines zentralen Dashboards.

**Jetzt kostenlos testen.**

SOLARWINDSMSP.COM/DE

solarwinds msp

Fußnoten:

[1] „Mobile Device Security: Startling Statistics on Data Loss and Data Breaches", ChannelPro Network. http://breachlevelindex.com/assets/Breach-Level-Index-Report-2016-Gemalto.pdf (Aufruf im Juli 2017).

[2] „Phishing by the Numbers: Must-Know Phishing Statistics 2016", Barkly https://blog.barkly.com/phishing-statistics-2016 (Aufruf im Juli 2017).

[3] https://www.av-test.org/en/statistics/malware/ (Aufruf im Juli 2017).

[4] „The 2016 Duo Trusted Access Report", Duo Security https://duo.com/assets/ebooks/duo-trusted-access-report.pdf (Aufruf im Juli 2017).

[5] „Domain Use and Trends", APWG. https://apwg.org/resources/apwg-reports/domain-use-and-trends (Aufruf im Juli 2017).

[6] „M-Trends 2015: A View from the Front Lines", Mandiant. https://www2.fireeye.com/WEB-2015-MNDT-RPT-M-Trends-2015_LP.html (Aufruf im Juli 2017).