



LIVE-HACKING

Praxisbeispiele & Schutzmaßnahmen



WHOAMI?



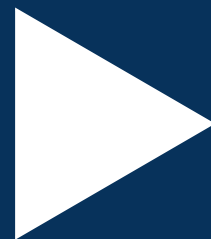
Falk Trümner

Senior Presales Consultant
DriveLock SE



Jean Pereira

Co-Founder / Head of Technology
SECBIZ IT Security GmbH



LIVE HACKING



FACTS



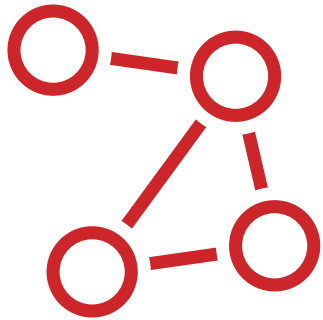
Cybercrime

ist ein sehr lukratives Geschäft



1.5 Billionen \$

Gewinn durch Cybercrime
im Jahr 2018



Angriffe

erfolgen immer häufiger
und werden immer komplexer

SCHADSOFTWARE INSGESAMT 2010 - 2019



Letzte Aktualisierung: 13. September 2019

Copyright © AV-TEST GmbH, www.av-test.org

ANTI-VIRUS ERKENNUNGSRATE



✓ No engines detected this file



1581e12962cecdccc1cc3f5a980e8a3b74da95cc5f0edf9fdd8607e33a8a882b

534.7 KB
Size

2019-08-24 11:38:46 UTC
27 days ago



USBLogView

overlay peexe signed



Community
Score





99%

Aller Cyberattacken starten
mit einer Benutzerinteraktion



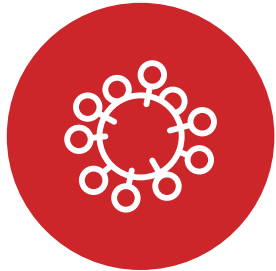
Jeder ist ein Ziel

Es stellt sich nicht die Frage ob,
sondern wann man angegriffen wird.

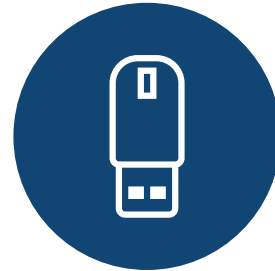


SCHUTZMASSNAHMEN

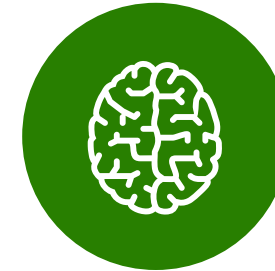
HANDLUNGSEMPFEHLUNG



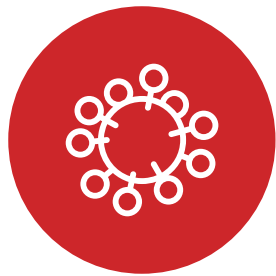
Effektiver Schutz gegen bekannte und unbekannte Schadsoftware



Restriktive Verwendung von externen Laufwerken und Geräten



Sensibilisierung der Anwender für IT-Sicherheit



Effektiver Schutz gegen bekannte
und unbekannte Schadsoftware

DRIVELOCK APPLICATION CONTROL



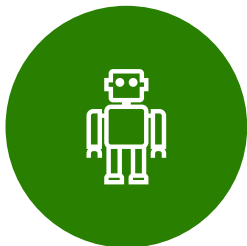
Schutz vor Schadsoftware

Durch Application Whitelisting hat jegliche dateibasierte Schadsoftware keine Chance ausgeführt zu werden – ob bekannt oder unbekannt. Das Prinzip eines Antivirus wird umgekehrt und nur genehmigte Software zugelassen.



Kontrolle über Applikationen

Egal ob Skriptinterpreter, Zugriffe auf das Dateisystem, die Windows Registrierung oder systemeigene Tools, die für Angriffe genutzt werden können – Sie haben die volle Kontrolle über sämtliche Berechtigungen.



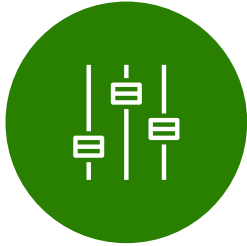
Intelligente Lernmodi

Softwareverteiler- oder Patchmanagementsysteme können zur automatischen Genehmigung integriert werden. Für manuelle Softwareinstallationen stehen verschiedene Lernmodi für eine einfache Administration zur Verfügung.



Restriktive Verwendung von
externen Laufwerken und Geräten

SMART DEVICEPROTECT



Kontrolle über sämtliche Geräte

Sie definieren, wer welche Geräte (Z.B. USB-Sticks, externe Festplatten, Smartphones etc.) in welchem Umfang verwenden darf.



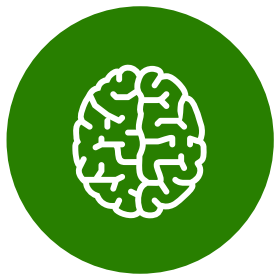
Schutz vor Datendiebstahl und Schadsoftware

Das Einschleusen von Schadsoftware, Datenabfluss oder Bad-USB Angriffe werden effektiv unterbunden.



Sichtbarkeit über die Gerätenutzung

Sämtliche Ereignisse werden ganzheitlich protokolliert. Wahlweise können von allen transferierten Dateien Schattenkopien erstellt werden.



Sensibilisierung der Anwender
für IT-Sicherheit

SMART SECURITYEDUCATION



Das richtige Wissen zur richtigen Zeit

Durch den event-basierten Ansatz erhalten Ihre Mitarbeiter das richtige Training, zur richtigen Zeit. Durch das kontinuierliche Lernen wird das Wissen dauerhaft verfestigt, bevor es vergessen wird.



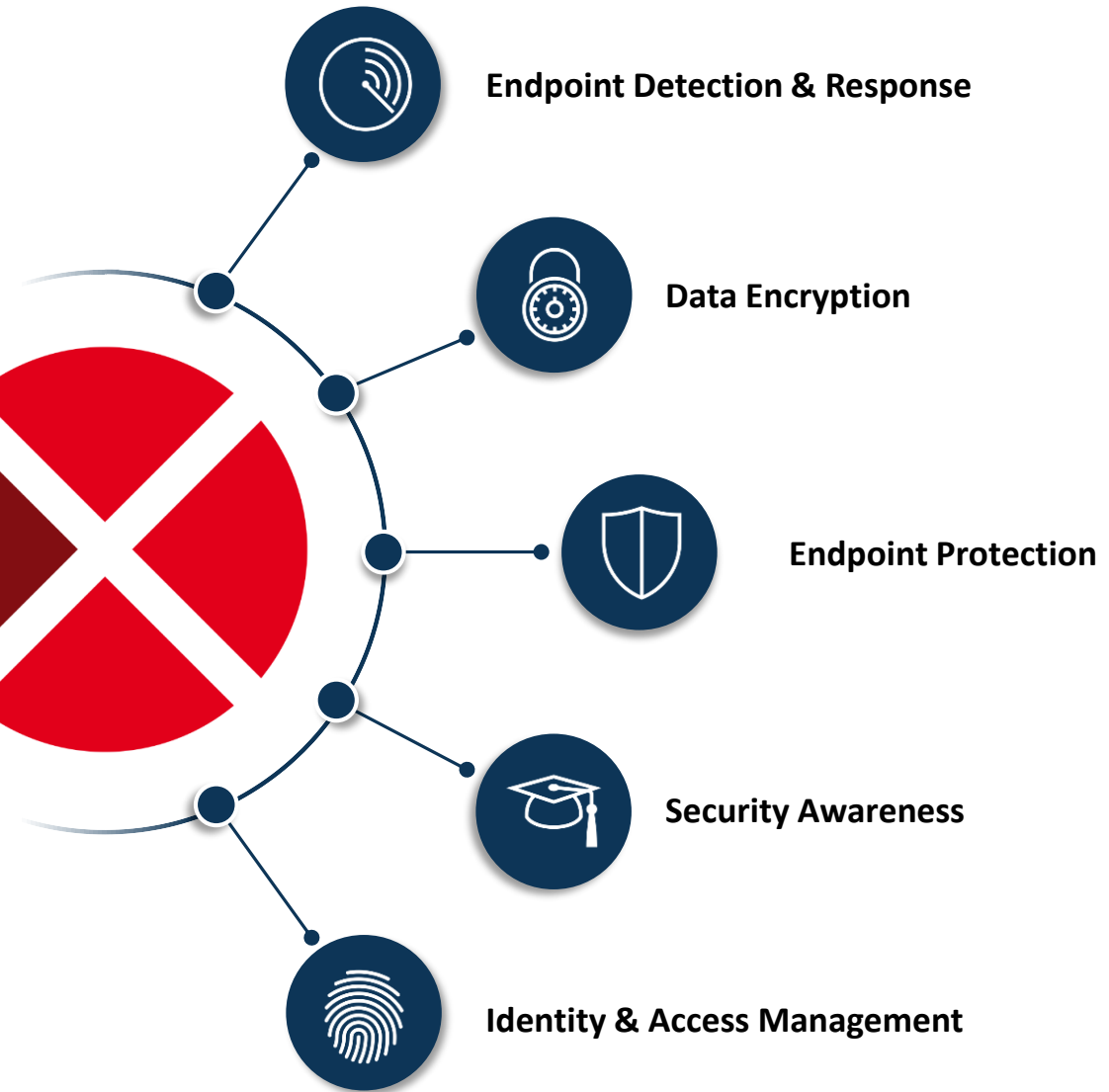
Umfangreiche und abwechslungsreiche Trainings

Neben eigenen Inhalten wie Dokumenten, Bildern, Videos oder Webinhalten können interaktive Lerneinheiten in unterschiedlichen Formaten aus einer umfangreichen Bibliothek mit über 30 Themen verwendet werden.



Volle Transparenz über den Lernerfolg

Sämtliche Fortschritte werden ganzheitlich protokolliert und können zentral ausgewertet werden. Wahlweise können von allen transferierten Dateien Schattenkopien erstellt werden.



VIELEN DANK!

**Besuchen Sie uns!
Halle 9 | Stand 9-230**



Falk Trümner

Falk.Truemner@drivelock.



SECBIZ

Jean Pereira

Pereira@secbiz.com