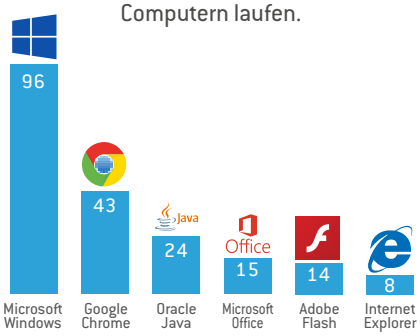
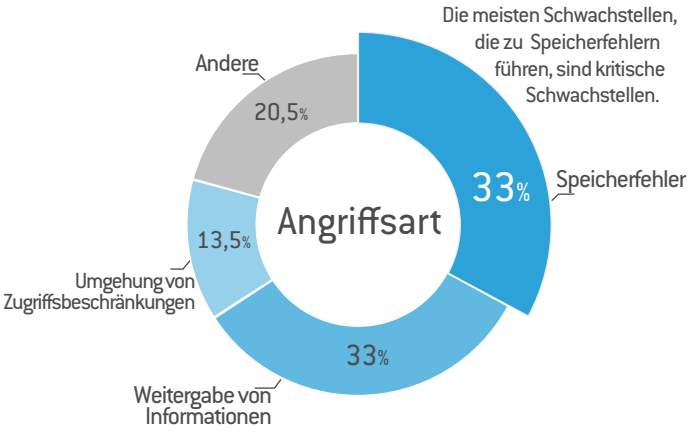
Endpoint Security Monitoring, Übersicht
Januar - Juni 2017

Von Stormshield analysierte Schwachstellen

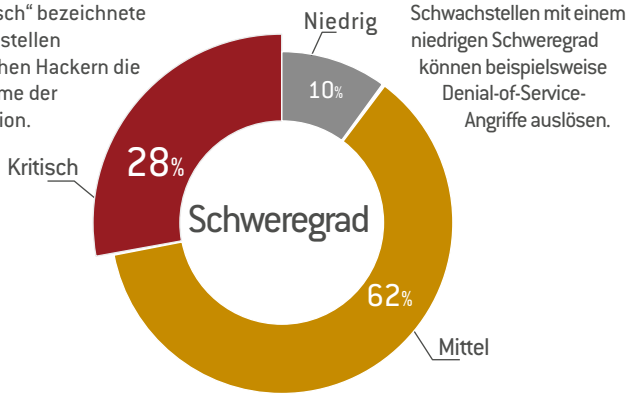
200
Schwachstellen wurden von unserem Security Monitoring-Team analysiert (Januar-Juni)

Diese Schwachstellen betreffen bekannte Softwareprodukte, die auf den meisten Computern laufen.





Die meisten Schwachstellen, die zu Speicherfehlern führen, sind kritische Schwachstellen.

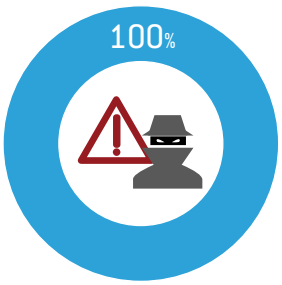


Als „Kritisch" bezeichnete Schwachstellen ermöglichen Hackern die Übernahme der Workstation.

Schwachstellen mit einem niedrigen Schweregrad können beispielsweise Denial-of-Service-Angriffe auslösen.

Von SES proaktiv blockiert

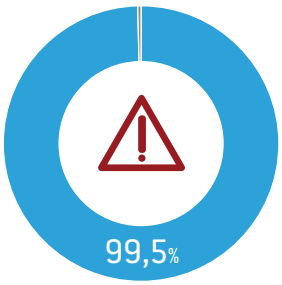
Stormshield SES blockierte proaktiv die meisten Exploits von Schwachstellen.
Wenn Schwachstellen nicht proaktiv blockiert werden, veröffentlicht SES einen Bericht mit Empfehlungen, wie die Systemrichtlinien anzupassen sind.



Bekannte*und kritische Exploits

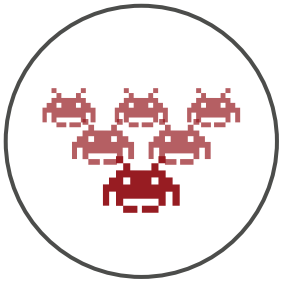
Stormshield SES blockierte 100 % kritischer Angriffe mit bekannten Exploits.

*„Bekannt" bezieht sich auf Exploits, die bereits beobachtet wurden



Kritische Exploits

AUCH WENN diese Schwachstellen nicht ausgenutzt wurden, würde SES 99,5% der Exploits kritischer Schwachstellen blockieren. Die restlichen würden durch die von Stormshield bereitgestellten Sicherheitsberichte abgedeckt.



Malware

SES blockiert AUCH Malware, die nicht notwendigerweise eine Schwachstelle ausnutzt. Beispiel: Die Ransomware Petya.B und Locky, Dridex-Angriffe, Cryptoblocker, Cryptowall und Teslacrypt.

STORMSHIELD

WWW.STORMSHIELD.COM

Stormshield, eine 100%-Tochter von Airbus Defence and Space, bietet innovative, durchgängige Sicherheitslösungen zum Schutz von Netzwerken (Stormshield Network Security), Computern (Stormshield Endpoint Security) und Daten (Stormshield Data Security) an.