IT Sicherheit: Virenschutz/Malwareschutz

Veröffentlicht: Donnerstag, 13. Sep 2018

Wie Sie bereits wissen, ist ein Virus für Ihren PC so ähnlich wie für Sie eine Grippe. Bei Malware handelt es sich um ein Programm das unerwünschte Funktionen ausführt. In beiden Fällen müssen Sie Ihren PC oder Server nicht zum Arzt bringen - wichtiger ist vielmehr ihn vor der Infektion zu schützen. Das können Sie tun, indem Sie ein Anti-Viren-Programm oder einen Viren-Scanner installieren. Unter Windows ist eine gute Antiviren-Software unerlässlich, da Windows-Rechner aufgrund ihrer weiten Verbreitung am häufigsten angegriffen werden. Für Linux und MAC OS X sind bislang kaum Schadprogramme bekannt, die „kommerziell“ genutzt werden.

Antiviren-Software überprüft neue Dateien (zum Beispiel Anhänge von E-Mails) und den gesamten Computer auf Anzeichen einer Infektion. Dazu vergleicht sie in erster Linie die Daten auf Ihrem Rechner mit den „Fingerabdrücken“ bekannter Schadprogramme. Diese „Signaturen“ müssen aber immer auf dem aktuellen Stand sein, weil täglich neue Varianten von Schädlingen auftreten. Deshalb müssen Sie die Software regelmäßig aktualisieren (updaten). Das geht über die automatische Update-Funktion Ihres Programms. Hinzu kommen Verfahren, die auch bislang noch unbekannte Schadprogramme finden sollen.

Schubert IT GmbH hilft Ihnen das für Sie und Ihre Bedürfnisse richtige Produkt zu finden und entsprechend Ihren Anforderungen zu implementieren. Als Anlage haben Wir Ihnen noch ein paar Stichworte zum Thema Virenschutz und Malwareschutz zusammengestellt. Bei Fragen rufen Sie uns gerne an Tel 04231 9566012 ,schreiben uns eine Mail an info@schubertservice.de oder benutzen unser Kontaktformular. Schubert IT GmbH - IT Sicherheit für Verden.

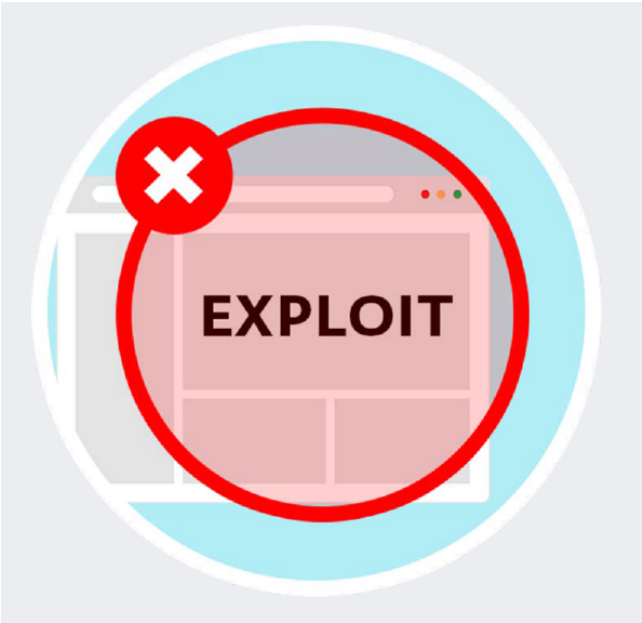


Antivirus und Antispyware

Eleminieren Sie Bedrohungen und Verhindern Sie die Ausbreitung von Malware auf andere Rechner.

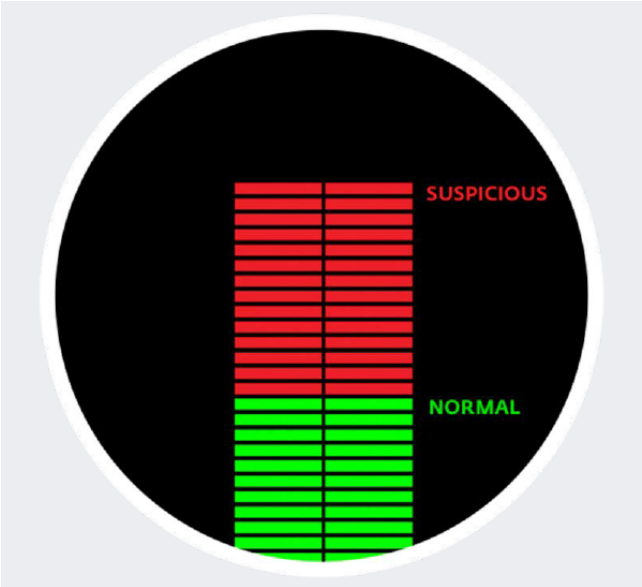
Exploit Blocker

Blockieren Sie Angriffe von getarnter Malware und schützen Sie sich vor Trojanern und Erpressersoftware Wehren Sie sich gegen Attacken auf Ihren Webbrowser, PDF Reader und andere Anwendungen, einschließlich Java – basierter Software.



Erweiterte Speicherprüfung

Erkennen und beseitigen Sie getarnte und verschlüsselte Malware, und überwachen Sie verdächtige Prozesse.



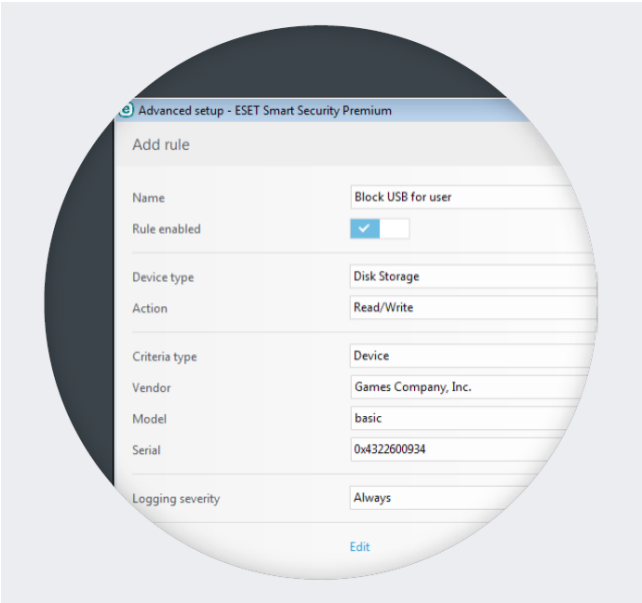
Cloudbasierter Scan

Setzen Sie vertrauenswürdige Dateien / Quellen und die dazugehörigen Ressourcen auf eine Whitelist. Wehren Sie Bedrohungen ab in dem Sie verhaltensbasierte Erkennung konfigurieren.



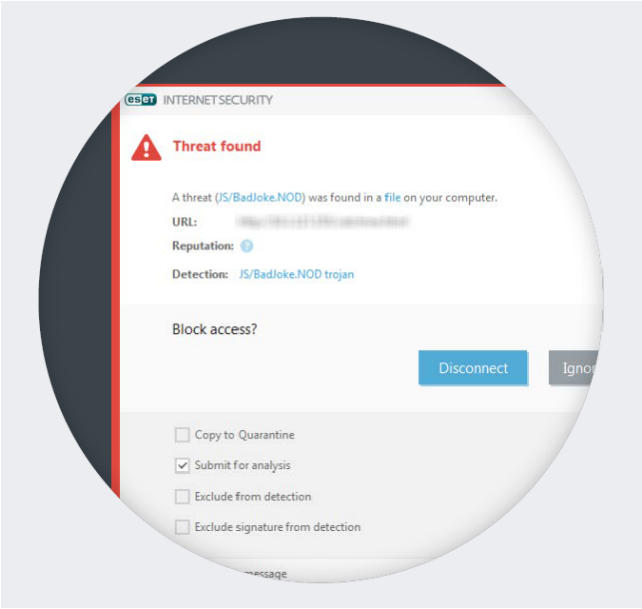
Hostbasierter Schutz vor Angriffen (HIPS)

Überwachen Sie Systemvorgänge und blockieren Sie verdächtige Interaktionen. Erstellen Sie Regeln für Ihre System Registry und überwachen diese entsprechend nach Ihrem Bedarf.



Schutz vor Skript-basierten Angriffen

Erkennen Sie gefährliche Skripte die versuchen Windows PowerShell auszunutzen. Entdecken und vermeiden Sie JavaScripts die Ihren Browser angreifen.



Prüfung von Downloads

Scannen Sie Dateien bereits während des Herunterladens (UEFI Schnittstelle)

Schützen Sie Ihre Privatsphäre

Schützen Sie Ihre Passwörter vor Missbrauch

Datenverschlüsselung

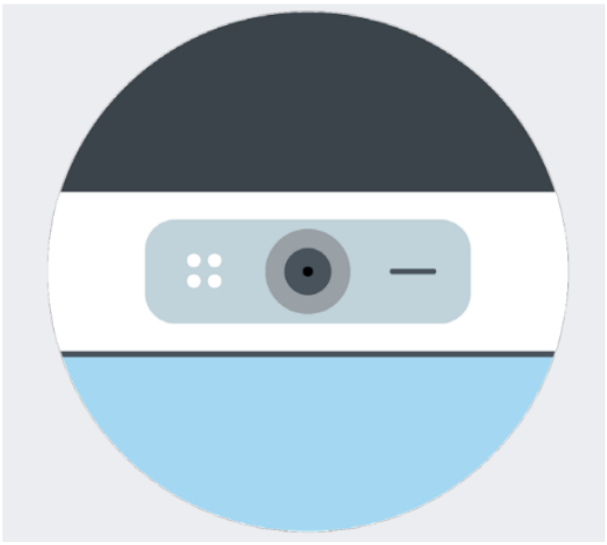
Verschlüsseln Sie Ihre Daten und Dateien auf Wechselmedien und sichern somit einen störungsfreien Datenaustausch.

Passwort Management

Benutzen Sie ein System zum Passwort Management und organisieren Sie Ihre Passwörter in einem System. Verwenden Sie unterschiedliche Passwörter.

Prüfen Sie auf laufende Prozesse

Prüfen Sie Ihre Systeme auf laufende Prozesse so das unerlaubte Zugriffe auf z.B. die Webcam nicht möglich sind.



Firewall

Konfigurieren Sie auf Ihren Systemen die Firewall und schützen Sie Ihre Systeme vor Zugriff und Datendiebstahl.

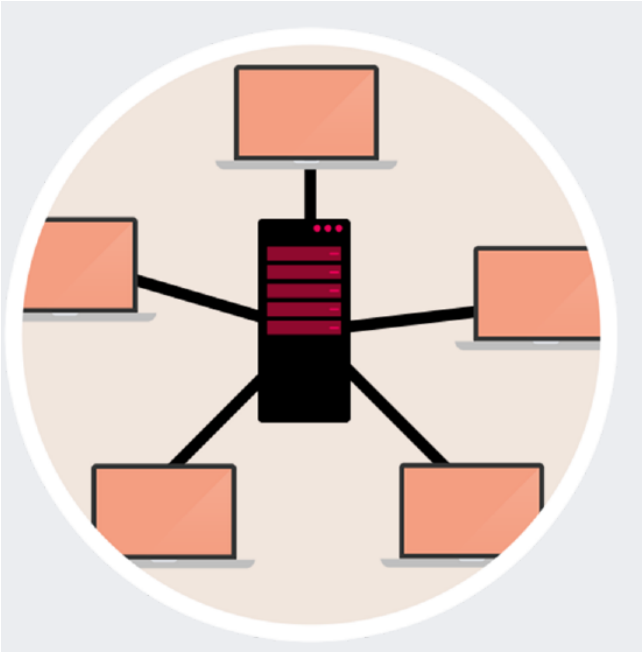
Sicheres online Banking

Verschlüsseln Sie die von der Tastatur an den Browser übermittelten Informationen und schützen Sich somit vor Keyloggern.



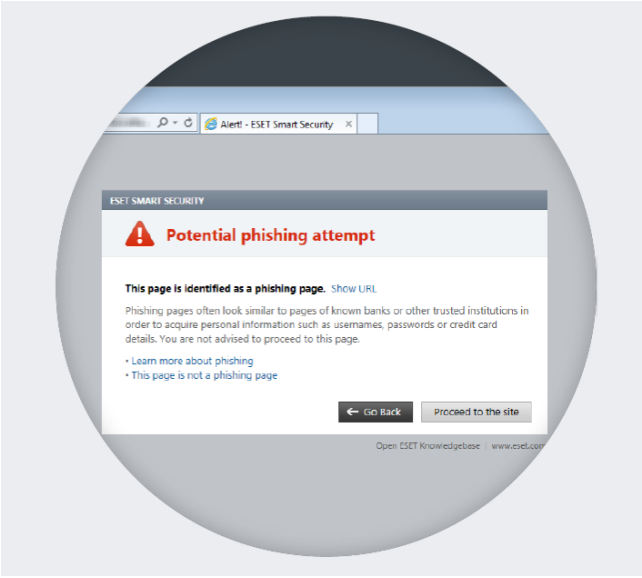
Botnet Erkennung

Verhindern Sie das Ihre Systeme von Kriminellen für die Verbreitung von Spam Angriffen gegen fremde Systeme oder für andere illegale Aktivitäten missbraucht wird. Schauen Sie sich die Netzwerksignaturen entsprechend genau an.



Anti-Phishing

Schützen Sie sich vor gefälschten Webseiten auf denen Ihre persönlichen Daten abgegriffen werden sollen.



Medienkontrolle

Verhindern Sie das unerlaubte Kopieren Ihrer Daten auf externe Geräte, sperren Sie gegebenenfalls die Verbindung zu Wechselmedien über Bluetooth FireWire und seriellen/parallelen Ports.

Antispam

Konfigurieren Sie Spamrichtlinien um Ihr Postfach von unerwünschter Post frei zu halten.



Link BSI Surftipps:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSIFB/Broschueren/Brosch_A6_Surfen_aber_sicher.pdf?__blob=publicationFile&v=4

Link BSI Virenschutzprogramme:

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Schutzprogramme/Virenschutzprogramme/virenschutzprogramme_node.html

Schubert IT GmbH Kontaktformular:

https://www.schubertservice.de/index.php/kontakt.html

Zurück