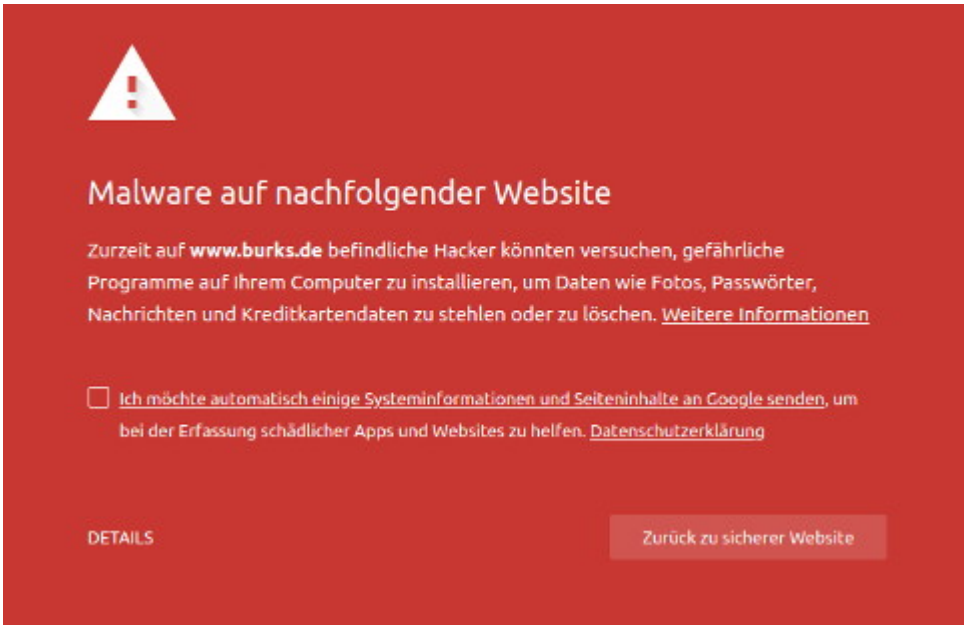
Es cybert sehr oder: Ich hacke euch alle!



Cyberattacken allüberall. Überraschung! Es war Putin – „according to people familiar with the matter." Schon klar.

Der Postillion hatte vor drei Jahren etwas dazu geschrieben.

Mal ganz langsam zum Mitschreiben. *All of the organizations were breached through the update server of a network management system made by the firm SolarWinds, FireEye said in a blog post Sunday.*

SolarWinds.Orion.Core.BusinessLayer.dll is a SolarWinds digitally-signed component of the Orion software framework that contains a backdoor that communicates via HTTP to third party servers. We are tracking the trojanized version of this SolarWinds Orion plug-in as SUNBURST.

Digital signiert, hmhm. Das müsste doch aufgefallen sein?

The backdoor uses multiple obfuscated blocklists to identify forensic and anti-virus tools running as processes, services, and drivers. Malware mit eingebautem Schlangenöl-Detektor!

Sehr witzig.

By the way: Was ist eigentlich eine dll-Datei?
DLL-Dateien verhalten sich ähnlich wie die bekannten EXE-Dateien. Die DLL-Dateien lassen sich per Doppelklick ausführen, jedoch läuft die Handlung meist unsichtbar im Hintergrund ab.
Die Dateiendung .dll wird nicht nur von DLL-Dateien, sondern auch von EXE-Dateien und Treibern genutzt. DLL-Dateien sind somit ein wichtiger Bestandteil des Windows-Systems.

Soso.