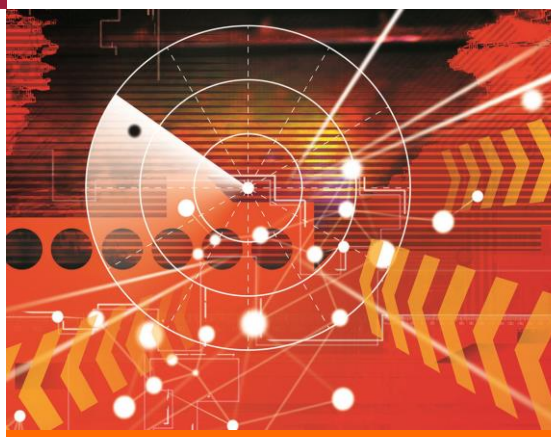
Krypto-Trojaner **WannaCry**

CGI
Experience the commitment®

Aktuelle Sicherheitsinformation



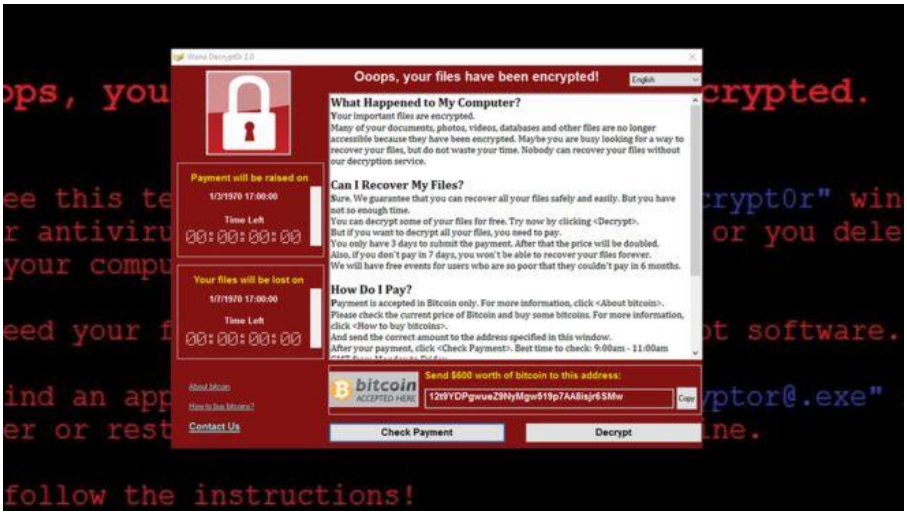
Der Krypto-Trojaner WannaCry verbreitet sich seit Freitag, 12. Mai 2017 09:24 Uhr deutscher Zeit rasant in den Computernetzen von mehr als 150 Ländern weltweit und verschlüsselt die befallenen Systeme.

DIE BEDROHUNG

Der zur Gruppe der Ransomware zählende Trojaner verbereitet sich in seiner Urversion per E-Mail, die nicht vollständig lesbar ist. Über ein Makro, das scheinbar die korrekte Darstellung (Decodierung) ermöglicht, wird der Schadcode auf den Rechner geladen. Im Wesentlichen enthält er zwei Teile

- Weiterverbreitung unter Ausnutzung des Exploits (siehe MS17-010).
- Dateiverschlüsselung und Bildschirmsperre auf befallenen Rechnern

Das folgende Bild zeigt die Meldung auf infizierten Computern.



DIE URSACHE

Der Krypto-Trojaner WannaCry nutzt einen der NSA zugeschriebenen Exploit namens EternalBlue, der am 14. April 2017 durch die Hackergruppe Shadow Brokers veröffentlicht wurde. Die im Microsoft Security Bulletin MS17-010 beschriebene Schwachstelle im veralteten SMB v1 Protocol wird ausgenutzt, damit sich WannaCry als Wurm weiter verbreiten kann.

DIE FOLGEN

WannaCry verschlüsselt die Daten der infizierten Systeme und fordert eine Zahlung von Lösegeld in Form von Bitcoins. Hierbei verdoppelt sich der Preis nach drei Tagen, nach sieben Tagen sollen die Daten gelöscht werden. Bei pünktlicher Zahlung sollen die Nutzer einen Code zur Entschlüsselung ihrer Daten erhalten.

FACTSHEET

WANNACRY & ABWEHR

Übersicht der Cybersecurity Lösungen:

Strategy, Compliance & Transformation

- Informationssicherheits- und Notfallmanagement
- Best Practices nach ISO 27001, ISO 25999, IT-Grundschutz und A-960/1
- Vulnerability Assessments und Penetration Testing
- Risikomanagementstrategien
- Aufbau von Sicherheitsprozessen
- Datenschutz und Datensicherheit
- Awareness Training

Secure Systems Engineering

- Sichere Netzarchitekturen
- Identity & Accessmanagement
- Sichere Softwareentwicklung
- Security Testing

Managed Security Services

- Managed Services
- Monitoring & Alerting
- SIEM as a Service
- Forensics & Malware Analysis
- Advanced Threat Intelligence

de.cgi.com/cybersecurity

Es sind u.a. betroffen:

- Krankenhäuser, die ihre Patienten aus der Notaufnahme wegschicken
- Automobilbauer wie Peugeot, deren Produktion tagelang still steht
- Transportdienstleister wie die Deutsche Bahn mit Ausfall der Anzeigen

DIE GRÜNDE

Einfach gesagt gibt es zwei Versäumnisse der Nutzer befallener Rechner:

1. **Mangelnde Awareness**
   Nutzer klicken zu schnell auf Links oder Attachments von E-Mails unbekannter Absender.
2. **Fehlende Updates und veraltete Systeme**
   Microsoft hat gegen die Lücke am 14. März 2017 Patches veröffentlicht. Allerdings wurden diese Patches für nicht mehr unterstütze Windows-Systeme erst am 12. Mai 2017 veröffentlicht.

AD HOC GEGENMASSNAHMEN

Sollte ein Patchen von Windows-Systemen nicht zeitnah möglich sein, gibt es folgende Möglichkeiten, um das Risiko einer Infektion zu reduzieren:

- Aktueller Malwareschutz: Der Windows Defender hat seit dem 12. Mai 2017 Signaturen für Ransom:Win32/WannaCrypt.
- Intrusion Prevention Systeme: Das IPS Snort hat seit dem 12. Mai entsprechende Regeln, das IPS Suricata seit dem 13. Mai.
- Eingebauter Kill-Switch: Erste Versionen von WannaCrypt verfügen über einen Mechanismus, der die Funktion einstellt, wenn die URL „iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com“ direkt per GET erreicht werden kann. Diese Domain ist seit dem 12. Mai registriert.
- Netzwerksegmentierung: Durch Schließen der für SMB-Freigaben notwendigen Ports an den Netzgrenzen, über die keine Freigaben erlaubt sein sollten, kann die Verbreitung eingeschränkt werden,

PRÄVENTIVER SCHUTZ

- Durchführung Awareness-Kampagnen und Vulnerability Assessments
- Optimierung des Patch-Managements und des Malware-Schutzes unter Gesichtspunkten des Risikomanagements
- Design und Implementierung einer vor Krypto-Trojanern sicheren Backup-Infrastruktur
- Sichere Netzwerksegmentierung mit Isolation und Migration von Altsystemen
- SIEM Services aus unseren Security Operation Centern (SOC) zur zeitnahen Erkennung und Analyse von Angriffen
- Vorbereitung von Gegenmaßnahmen, damit z.B. Intrusion Prevention Systeme (IPS) neben Hersteller-Regeln nach der Analyse des SOCs mit weiteren Ad-Hoc Regeln ausgestattet werden können

CGI berät Sie hierzu gerne und bietet in Kürze einen komplett deutschsprachigen SOC Service, denn

“Cybersecurity is part of everything we do.”

ÜBER CGI

Mit 70.000 Mitarbeitern an 400 Standorten in 40 Ländern übernimmt CGI vor Ort Verantwortung für den Erfolg seiner Kunden und bietet ihnen gleichzeitig globale Lieferfähigkeit. Seit unserer Gründung im Jahr 1976 pflegen wir eine strikte Lieferdisziplin, dank der unsere Projekte in Bezug auf Zeit- und Budgettreue in der Branche führend sind. Mit Business und IT Consulting, Systemintegration sowie Outsourcing Services auf höchstem Niveau unterstützt CGI seine Kunden dabei, laufende Investitionen besser zu nutzen und gleichzeitig neue Technologie- und Business-Strategien einzusetzen, mit denen sich optimale Lösungen für die gesamte Wertschöpfungskette erreichen lassen.

Das Resultat unseres Commitments zeigt sich im gemessenen Kundenzufriedenheitswert, der in den vergangenen zehn Jahren durchgängig mehr als 9 von 10 möglichen Punkten betrug.

IHR ANSPRECHPARTNER

CGI Deutschland Ltd. & Co. KG

Practice Cybersecurity

(Practice Head: **Frank Reiländer**)

Ettore-Bugatti-Straße 6-14
51149 Köln
T: +49 2203 6993 1050

Für weitere Informationen kontaktieren Sie uns unter csi@cgi.com
oder besuchen Sie uns auf de.cgi.com/cybersecurity.

de.cgi.com/cybersecurity