PETRWRAP: NACHFOLGER VON WANNACRY UND PETYA

Veröffentlicht am 28. Juni 2017 von Judith

Petrwrap: Gestern Mittag gab es zahlreiche Angriffe auf Computer Netzwerke weltweit. Bisher unbekannte Hacker infizierten PCs über eine Lücke im Betriebssystem von Windows. Die Erpresser fordern 300 US Dollar Lösegeld in der Digitalwährung Bitcoin. Europol ermittelt.

Wer hinter dem Angriff steckt ist noch unklar. Auch sind sich IT-Techniker nicht einig, ob es sich um die schon bekannte Ransomware „Petya“ handelt, die schon 2016 ihr Unwesen trieb oder um einen neuen Virus. IT-Sicherheitsforscher von Kaspersky, einer großen IT-Sicherheitsgesellschaft, sind sich sicher es handelt sich um den Virus Petrwrap. Abgeleitet von der Ransomware Petya funktionieren beide Viren ähnlich. Gefährlich ist Petrwrap, da nur 61 Antivirensoftwares die Ransomware erkennen und vor ihr warnen.

Ähnlich wie schon im Mai, als „WannaCry“ hunderttausende Computer in mehr als 150 Ländern befiel, unter anderem die Netzwerke von Renault und der Deutschen Bahn, infiziert auch Petya die Betriebssysteme von Großkonzernen.

WER IST ALLES BETROFFEN?

Zu den Opfern von Petya gehören in der Ukraine momentan die Ukrtelecom, die Nationalbank, drei weitere Banken, der Energieversorger Kiewenergo und Ukrenergo. Weitere Opfer in der Ukraine sind der Medienkonzern TRK und die Radiostationen Radio Lux und Radio Maximum.

Außerdem ist das seit 1986 havarierte Atomkraftwerk Tschernobyl betroffen. Die Kontrolle der

Radioaktivität findet momentan manuell statt. Laut der ukrainischen Polizei seien mindestens 22 Konzerne in der Ukraine betroffen.

In Russland meldete die Zeitung *Wedomosti* und der Ölkonzern *Rosneft* einen Befall Ihrer Betriebssysteme.

Laut der Süddeutschen Zeitung sind auch viele westliche Firmen betroffen, unter anderem die Deutsche Post, die Metro und Beiersdorf (Nivea).

Andere Unternehmen in Kopenhagen, Containerreederei Maersk, der Schweizer Nahrungsmittelkonzern Mondelez International (Milka), die Anwaltskanzlei DLA Piper in Madrid, US Pharma Konzern Merck und die Werbeagentur WPP aus England wurden zum Opfer von Petrwrap. Russland und die Ukraine sind von Petrwrap am heftigsten betroffen, allerdings meldeten auch Unternehmen in Deutschland, Polen, Italien, Großbritannien, Frankreich und den USA ein Befall Ihrer Betriebssysteme. Das genaue Ausmaß ist noch unklar!

WIE KONNTE DIE RANSOMWARE PCS INFIZIEREN?

Dazu, wie der Virus die PCs infizieren konnte, weiß man allerdings noch nichts. Ursprünglich hat der US Abhördienst NSA die Sicherheitslücke im Windows Betriebssystem ausgenutzt, um Informationen von Privatpersonen, sowie Unternehmen abzugreifen. Der NSA Code „Eternal Blue“ wurde von Hackern entdeckt und unter dem Pseudonym Shadow Brokers bedienten sich die Hacker an dem Code und erschufen WannaCry. Auch Petrwrap enthält Codeschnipsel von Eternal Blue. Zwar gibt es schon seit Monaten ein Update, indem Windows User genau diese Sicherheitslücke schließen können, aber anscheinend hatten die Betroffenen dieses Update noch nicht durchgeführt.

LÖSEGELDFORDERUNG

Wenn der PC von Petrwrap infiziert ist, wird der Nutzer aufgefordert 300 US Dollar in Bitcoin Währung zu überweisen, um dann eine persönliche ID und die Nummer des Bitcoin Wallets an eine E-Mail-Adresse der Berliner Firma Posteo. Posteo erlaubt die Registratur von komplett anonymen E-Mail-Adressen. Mittlerweile hat Posteo den Erpresser Account gesperrt.

WIE KANN MAN SICH SCHÜTZEN?

Das Bundesamt für Sicherheit und Technik rät um sich zu schützen, alle IT-Systeme auf den neusten Stand zu bringen. Arne Schönbohm, Amtspräsident des BSI alarmiert: "Angesichts der akuten Bedrohungslage rufen wir die Wirtschaft erneut dazu auf, die Risiken der Digitalisierung ernst zu nehmen und notwendige Investitionen in die IT-Sicherheit nicht aufzuschieben".

Wenn ihr noch weitere Fragen zum Thema Ransomware habt und wie ihr Euch schützen könnt, schaut doch mal in unseren Blog. Ransomware Trojaner Virus – was steckt hinter Locky, WannaCry & Co.

Natürlich könnt ihr uns bei Fragen auch immer kontaktieren. Die Media Company hilft Euch gerne weiter!