

Kloertext

Updates müssen kommen

journal.lu - 26.07.2017



„Aktualisierte und saubere Systeme sind essentiell“, Sam Grüneisen, Mitglied Chaos Computer Clubs.
SAM GRÜNEISEN

Nach einer erneuten Welle an Angriffen durch Crypto-Trojaner und andere Schädlinge, die teilweise auf längst geschlossene Sicherheitslücken setzen, fordern viele Experten eine Nachbesserung der Sicherheitskultur bei Unternehmen, aber auch bei den Privatanutzern. So ist erst am gestrigen Mittwoch die italienische Großbank Unicredit Ziel eines Hackerangriffs geworden. Rund 400.000 Menschen in Italien dürften betroffen sein - Passwörter und Kontonummern inklusive. Schädlinge und Würmer wie „WannaCry“ oder der „Petya“-Schädling veranschaulichen, dass es vielerorts immer noch an den grundsätzlichen Update-Mechanismen fehle, meint auch der Chaos Computer Club aus Luxemburg.

„Was wir bei den rezenten Fällen immer wieder gesehen haben ist der Umstand, vor dem wir schon seit Jahren warnen: Sicherheitsupdates werden einfach nicht zeitnah durchgeführt, was Schädlingen erlaubt, Systeme zu infizieren, die eigentlich längst sicher sein sollten. Besonders ärgerlich ist das, wenn die Lücke bereit seit Jahren gestopft ist, das Update aber trotzdem nicht appliziert wurde. Das war jetzt bei den rezenten Infektionen nicht der Fall, passiert aber trotzdem immer noch zu häufig. Deshalb fordern wir auch weiterhin: Systeme sind auf dem aktuellsten Stand zu halten - alles andere ist nicht einmal ansatzweise sicher, und wird besonders leicht zu einer Virenschleuder, die auch den Rest des Netzwerkes befällt, wie wir im Fall „WannaCry“ sehen konnten.

Wir sind natürlich realistisch: Nicht immer lassen sich Systeme zeitnah updaten, oft ist es auch eine Kostenfrage - oder es scheitert daran, dass der Hersteller einfach keine Updates mehr nachreicht. Das passiert etwa derzeit besonders oft bei den modernen smarten Haushaltsgeräten („Internet of Things“), deren Hersteller beim Erscheinen neuer Geräte oft einfach den Support einstellen. Wenn diese aber ähnlich wie Geldautomaten und alle anderen Rechner ständig am Internet hängen, sind auch sie für Angriffe verwundbar - hier müssen die Hersteller und die Nutzer gleichermaßen in die Pflicht genommen werden, ihre Updates auch auszuliefern und aufzuspielen. Der CCC Luxemburg setzt sich daher zusammen mit EDRI („European Digital Rights“) auf Europa-Ebene dafür ein, dass die Hersteller stärker verpflichtet werden, auch tatsächlich Updates anzubieten.

Zugleich leisten wir auch im Großherzogtum ständige Aufklärungsarbeit, kooperieren etwa mit SECURITYMADEIN.lu oder dem CIRCL, um bei solchen Fragen Hilfeleistung zu bieten. Trotzdem konzentrieren wir uns besonders auf die EU-Ebene, weil wir dabei mehr ausrichten können. Sogenannte „Krypto-Parties“, bei denen wir den Nutzern eine Verschlüsselung ihrer Daten aus Sicherheitsgründen anraten, organisieren wir aber trotzdem. Insgesamt gilt: Die Updatekultur muss sich ändern. Nur ein aktualisiertes Gerät ist wirklich sicher. Nicht nur für den einzelnen Rechner: Weil alles miteinander vernetzt ist, betrifft ein infizierter Rechner uns alle.“

- [Kloertext](#)