Fortschrittliche Angriffe – dynamische Entwicklung

Das BSI beobachtet jeden Tag die Bedrohungslage, die von neuen Schadprogrammen, erweiterten Angriffsmethoden oder gezieltem Vorgehen von Tätern für Unternehmen und Behörden ausgeht. In der jüngsten Zeit haben sich die Expertinnen und Experten im BSI-Lagezentrum und bei CERT-Bund zunehmend mit ausgefeilten Angriffstechniken auseinandersetzen müssen: Neue fortschrittliche Angriffe stellen ein vielfach höheres Bedrohungspotenzial dar, wenn sie beispielsweise in ein Unternehmensnetzwerk eindringen konnten. Eine Gesamtübersicht zum Thema Ransomware finden Sie unter **› Fakten und Abwehrstrategien**.

Digitale Erpressung mit Ransomware

Ransomware in seinen unterschiedlichen Varianten zielt in der Regel auf die Verschlüsselung von Nutzerdaten ab. Das Vorgehen der Täter zählt zu den fortschrittlichen Angriffen, deren Weiterentwicklung das BSI seit Jahren beobachtet. Nachdem Daten verschlüsselt wurden, wird ein Lösegeld erpresst. Die Daten werden erst nach Zahlung des meist digitalen Lösegelds wieder freigegeben, jedoch gibt es trotz Zahlung keine Garantie einen passenden Schlüssel zu erhalten. Mit Ransomware wurden bereits die unterschiedlichsten Organisationen Opfer eines Erpressungsversuchs: Großkonzerne, mittelständische Unternehmen bis hin zu Krankenhäusern.

Hohe Schäden durch Emotet

Das Schadprogramm **Emotet** stellt einen möglichen Angriffsvektor dar. Es ist in der Lage, Kontaktbeziehungen aus Mail-Postfächern auszulesen und in der Folge automatisiert sehr authentische Spam-Mails zu verschicken. Die Folge ist ein hoher Verbreitungsgrad bei gleichzeitig vergleichsweise hoher Erfolgsquote bei der Infizierung von Unternehmensnetzwerken. Emotet und nachgeladene Malware haben so bereits hohe Schäden bei Betroffenen in Wirtschaft und Verwaltung verursacht – und tauchen regelmäßig mit neuen Funktionen wieder auf, um ergänzt durch weitere Techniken und Schadsoftware Schaden anzurichten.

Immer neue Schadfunktionen

Fortschrittliche Angriffe zeichnen sich dadurch aus, dass sie Schadfunktionen, die früher bei ausgewählten Angriffen manuell eingesetzt wurden, heute breitflächig halbautomatisiert eingesetzt werden. Durch eine Vielfalt an Schadfunktionen geht von den fortschrittlichen Varianten eine deutlich größere Bedrohung aus. Neben der weiten Verbreitung durch immer bessere Spam-Mails durch Schadprogramme wie Emotet, gehen die Täter in vielen Fällen mittlerweile stufenweise vor. Während vor einiger Zeit noch einzelne Computer verschlüsselt wurden und Lösegeld pro verschlüsseltem PC verlangt wurde, werden heute betroffene Unternehmensnetzwerke zunächst gezielt ausspioniert. Dabei werden oftmals Daten ausgeleitet und eine Bewertung des jeweiligen Opfers vorgenommen. Die Täter passen ihre Lösegeldforderung dann der betroffenen Organisation an. Die Verschlüsselung erfolgt oftmals gezielt und kann dabei auch vorhandene Back-ups umfassen. Die Unternehmensnetzwerke sind häufig vollständig kompromittiert. Die zuvor ausgeleiteten Daten werden oftmals zur Erhöhung des Handlungsdrucks bei den Opfern eingesetzt, indem eine Veröffentlichung oder ein Weiterverkauf der Daten angedroht wird, sollte das Lösegeld für die verschlüsselten Daten nicht gezahlt werden. Die Bereinigung der betroffenen Netzwerke kann abhängig von der Größe des betroffenen Netzwerks Monate in Anspruch nehmen. Zuletzt wurde in mehreren Fällen bei Nicht-Zahlung mit der Veröffentlichung von zuvor gestohlenen Daten gedroht und teilweise auch durchgeführt.
Vor diesem Hintergrund wird konsequentes präventives Handeln immer wichtiger. Das BSI hat die Bewertung der Lage sowie die wichtigsten präventiven Maßnahmen in folgenden Dokumenten zusammengefasst.
Wenn es bereits zu einem **› IT-Sicherheitsvorfall** gekommen ist, hat das BSI zahlreiche Erste-Hilfe-Maßnahmen zusammengestellt.

Zum Thema

- **Ransomware Angriffe**
- **Ransomware – Vorsicht vor Erpressersoftware**
- **Download Ransomware: Managementabstract Fortschrittliche Angriffe (PDF)**
- **Download Ransomware: Bedrohungslage 2022 (PDF)**
- **Download Maßnahmenkatalog Ransomware (PDF)**
- **Download Ransomware: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall Version 1.2 (PDF)**
- **Emotet**

Ähnliche Themen

Social Engineering | APT | Malware | DDoS

Zurück zu Cyber-Sicherheitsempfehlungen nach Gefährdungen

Kurz-URL: https://www.bsi.bund.de/dok/fortschrittliche-angriffe

Seite drucken