Karlsruher Institut für Technologie

IT-Sicherheitsbeauftragter
Andreas Lorenz

DSB
Datenschutzbeauftragte
Ass. jur. Marina Bitmann

Datum: 12.02.2016

Zertifikat seit 2010
audit familiengerechte hochschule

Der IT-Sicherheitsbeauftragte und die Datenschutzbeauftragte informieren:

Liebe Kolleginnen und Kollegen,

immer wieder erreichen das KIT E-Mails mit Schadsoftware, die das Ziel haben, die Rechnersysteme zu infizieren. In der letzten Vergangenheit häufen sich aber Fälle mit sogenannter Verschlüsselungsschadsoftware (Ransomware), welche gleich in mehrfacher Hinsicht Schaden verursachen. Durch diese Schadsoftware können Daten nicht nur in unberechtigte Hände gelangen, sondern es werden die Originaldaten auf den befallenen Systemen verschlüsselt und somit für Sie unzugänglich gemacht. Das betrifft sowohl lokal abgelegte Daten als auch auf extern angeschlossenen Datenträgern bzw. Netzlaufwerken gespeicherte Daten. Die Angreifer bieten an, gegen Bezahlung einer Lösegeldsumme (i.d.R. ca. 500 € in BitCoins) die für die Entschlüsselung notwendigen kryptographischen Schlüssel zur Verfügung zu stellen. Sollte nicht bezahlt werden, dann bleiben diese Daten unlesbar. Es gibt derzeit kein Werkzeug, das die Daten in diesem Fall wiederherstellen kann.

Die Angreifer haben bereits gedroht, bei Nichtbezahlung die verschlüsselten Daten im Klartext im Internet zu veröffentlichen.

Eine Garantie, dass man bei Bezahlung den Schlüssel erhält und die Daten wieder entschlüsseln kann, gibt es nicht. Es gibt auch keine Garantie dafür, dass man mit der Zahlung die Veröffentlichung der Daten verhindert.

Je nach Art und Sensibilität der Daten kann ein solcher Angriff für das KIT einen sehr hohen Schaden bedeuten, insbesondere dann, wenn es sich um Daten mit einem hohen Schutzbedarf handelt. Werden personenbezogene Daten im Internet veröffentlicht, handelt es sich um eine massive Datenschutzverletzung, die für das KIT schwere Folgen haben kann.

Die Angreifer gehen sehr geschickt vor, um die potentiellen Opfer zur Ausführung der Schadsoftware zu verleiten. Wir konnten beobachten, dass die Anschreiben (Phishingmails) sehr sorgfältig erstellt wurden. Beispielsweise wird vorgetäuscht, dass man sich auf eine tatsächlich vorhandene Stellenausschreibung hin meldet, um ein infiziertes Dokument zur Ausführung durch den Empfänger zu bringen („Spear-Phishing“).

Durch das Ansehen des Dokuments (z.B. PDF, DOC, XLS) gelangt die Schadsoftware auf den Rechner und lädt danach weitere aktualisierte Schadsoftware nach.

Daher gilt im Umgang mit E-Mails Folgendes zu beachten:

- Öffnen Sie keine E-Mail-Anhänge, die Ihnen merkwürdig vorkommen oder die Sie nicht erwarten.
- Öffnen Sie auch keine E-Mail-Anhänge von Ihnen bekannten Personen, wenn in den Nachrichten nicht explizit auf die Anhänge verwiesen wird. Schädliche Links und Dateien können auch von Kolleginnen und Kollegen im KIT versendet werden, wenn deren Rechner oder deren KIT-Account kompromittiert wurden.
- Klicken Sie keine dubiosen Links an, die Sie in E-Mails finden. Prüfen Sie generell bei allen Links genau, ob Sie wirklich auf die Seite verlinken, die im Text angegeben ist.
- Seien Sie skeptisch, wenn unerwartet Rechnungen, Bewerbungen oder Schreiben von Anwälten per E-Mail ankommen. Oft werden auch E-Mails von großen deutschen Telekommunikationsunternehmen und Banken gefälscht. Diese sind sowohl vom Design als auch vom Text her kaum von den Originalen zu unterscheiden.
- Falls seltsam anmutende E-Mails und E-Mails mit Dateianhängen von bekannten Absendern bei Ihnen ankommen, fragen Sie bei den Absendern nach bzw. informieren Sie sie darüber, dass ihr Rechner eventuell automatisch Mails versendet.

Um für die Arbeit wichtige Daten nicht zu verlieren und die Anforderungen an die Verfügbarkeit der Daten zu erfüllen gilt zusätzlich Folgendes zu beachten:

- Es muss gewährleistet sein, dass die für Ihre Arbeit benötigten Daten einer ordentlichen Datensicherung unterliegen (Backup).
- Es muss sichergestellt sein, dass die Arbeitsrechner mit aktualisierter Software ausgestattet sind (Patches).
- Es muss gewährleistet sein, dass die Systeme mit aktueller Antiviren-Software ausgestattet sind.

Wenden Sie sich bei verdächtigen E-Mails an die/den für Ihre OE zuständigen IT-Beauftragte/n (ITB) oder an das KIT-CERT (cert@kit.edu).

Andreas Lorenz
IT-Sicherheitsbeauftragter

Marina Bitmann
Datenschutzbeauftragte