Interview
Betrug rechtzeitig erkennen

[26.2.2018] Welche Gefahr Cyber-Attacken auf Behörden darstellen und wie ihr begegnet werden kann, erläutert Carsten Maßloff, Geschäftsführer von Ceyoniq Technology, im Interview. Seine Überzeugung: Informationssicherheit ist ein Thema für die Entscheiderebene.

Herr Maßloff, das Land Nordrhein-Westfalen möchte im Kampf gegen Cyber-Kriminelle enger mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zusammenarbeiten (wir berichteten). Warum war dieser Schritt notwendig?

Die Bedrohungslage für Behörden hat sich in der jüngeren Vergangenheit spürbar verschärft. Einerseits gefährden stetig neue Varianten von Schad-Software die Informationssicherheit von Behörden. Andererseits gehen die Angreifer zu immer raffinierteren Methoden über, um Firewalls und andere Sicherheitsmaßnahmen zu umgehen. Sie zielen vermehrt auf die Unwissenheit der Mitarbeiter ab und versuchen, diese mit ausgeklügelten Betrugsszenarien zu verhängnisvollen Handlungen zu bewegen.

Können Sie dafür Beispiele nennen?

Zunächst sei hier das Spear-Phishing genannt, das bildlich an den Speer angelehnt ist. Dabei verfassen die Kriminellen äußerst echt anmutende E-Mails, die zu logisch nachvollziehbaren und dadurch vermeintlich harmlosen Aktionen auffordern. Die aufwendig gefälschten E-Mails bringen Empfänger letztlich wesentlich schneller dazu, Anhänge zu öffnen oder auf gefährliche Links zu klicken. Hinzu kommt der so genannte CEO-Betrug. Dabei geben sich die Kriminellen als Vorgesetzte eines Mitarbeiters aus. Zur Vorbereitung recherchieren sie die nötigen Informationen vorwiegend im Internet und weisen dann die ahnungslosen Sachbearbeiter zum Beispiel per E-Mail an, Überweisungen größerer Geldbeträge vorzunehmen.

Den Menschen in den Mittelpunkt der Maßnahmen zu stellen, ist der richtige Ansatz.

Müssten Behördenmitarbeiter den Betrug nicht erkennen?

Lassen Sie mich ein Beispiel aus dem BSI-Lagebericht 2017 anführen, der zeigt, dass die Betrugsmasche leider äußerst effektiv

ist: Die Mitarbeiterin einer Landesbehörde erhielt vom vermeintlichen Präsidenten des Amts per E-Mail die personalisierte Anweisung, eine "vertrauliche Finanztransaktion" in Höhe von 961.000 Euro vorzunehmen. Um der falschen Anweisung Nachdruck zu verleihen, fingierten die Betrüger sogar den Anruf einer angeblichen Anwältin.

Wie können sich Behörden effektiv gegen diese Art der Cyber-Kriminalität schützen?

Der Schlüssel zum Erfolg sind ganzheitliche technisch-organisatorische Maßnahmen, so genannte TOMs. Um die Mitarbeiter für die gestiegene Gefahrenlage zu sensibilisieren, empfiehlt sich zum Beispiel ein konkreter Katalog mit Verhaltensregeln. Ebenso sollten Schulungen und Audits von entsprechenden Experten durchgeführt werden. Den Menschen in den Mittelpunkt der Maßnahmen zu stellen, ist der richtige Ansatz. Auch ein besseres und zentrales Informationsmanagement ist ein wichtiger Punkt auf der Agenda. Der intensivere Austausch von Gefährdungsindikatoren, etwa über die vom Bund betriebene Malware Information Sharing Platform (MISP), ist dabei ein entscheidender Schritt. So können Betrugsfälle schneller registriert und weitere Institutionen vor einer neuen Angriffswelle gezielt gewarnt werden. Die Zusammenarbeit zwischen dem Land NRW und dem BSI ist daher ein wichtiges Signal: Informationssicherheit ist heute ein Thema, das auf Entscheiderebene verankert werden muss.

Interview: Malte Limbrock, PR-Berater in Bonn

http://www.ceyoniq.com

Stichwörter: IT-Sicherheit, Ceyoniq

Bildquelle: Ceyoniq Technology GmbH

Quelle: www.move-online.de