PRESSEMITTEILUNG

Informationssicherheit

Cyberkriminalität in NRW: „Den Menschen in den Mittelpunkt zu stellen, ist der richtige Ansatz“

Experten-Interview mit Carsten Maßloff, Geschäftsführer der Ceyoniq Technology GmbH, zur aktuellen Absichtserklärung von Land NRW und BSI

- Land NRW und BSI geben Absichtserklärung ab
- Neue Angriffsmethoden von Cyberkriminellen im Fokus
- Faktor Mensch als Schwachstelle

Düsseldorf / Bielefeld, 22.02.2018 – Gemeinsam gegen Cyberkriminelle: Das Land Nordrhein-Westfalen intensiviert die Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI). Ziel der gemeinsamen Absichtserklärung ist es, insbesondere Behördenmitarbeiter künftig besser gegen Cyberkriminalität zu schützen. Damit reagiert die Landesregierung auf die verschärfte Bedrohungslage. Laut BSI-Lagebericht 2017 häufen sich die Attacken auf Behörden, zudem haben es die Angreifer vermehrt auf den Faktor Mensch als Schwachstelle abgesehen. Carsten Maßloff, Geschäftsführer der auf Enterprise Content Management und Informationssicherheit spezialisierten Ceyoniq Technology aus Bielefeld, sieht in der engen Zusammenarbeit einen dringend notwendigen Schritt. Seine Einschätzung im Interview:

Frage: Herr Maßloff, das Land NRW möchte im Kampf gegen Cyberkriminelle enger mit dem BSI zusammenarbeiten. Was hat diesen Schritt notwendig gemacht?

Maßloff: Die Bedrohungslage für Behörden hat sich in der jüngeren Vergangenheit spürbar verschärft. Einerseits gefährden stetig neue Varianten von Schadsoftware die Informationssicherheit von Behörden. Andererseits gehen die Angreifer zu immer raffinierten 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.

Frage: Können Sie dafür Beispiele geben?

Maßloff: 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 aufwändig gefälschten Mails bringen Empfänger letztlich wesentlich schneller dazu, Anhänge zu öffnen oder auf gefährliche Links zu klicken. Hinzu kommt der sogenannte 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 Mail an, Überweisungen größerer Geldbeträge vorzunehmen.

Frage: Müssten Behördenmitarbeiter den Betrug nicht erkennen?

Maßloff: 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 Amtes per Mail die personalisierte Anweisung, eine „vertrauliche Finanztransaktion“ in Höhe von 961.000 Euro vorzunehmen. Um der falschen Anweisung zusätzlichen Nachdruck zu verleihen, fingierten die Betrüger sogar den Anruf einer angeblichen Anwältin.

Frage: Wie können sich Behörden effektiv gegen diese Art der Cyberkriminalität schützen?

Maßloff: Der Schlüssel zum Erfolg sind ganzheitliche technisch-organisatorische Maßnahmen (sog. TOMs). Um das Bewusstsein der Mitarbeiter für die gestiegene Gefahrenlage zu sensibilisieren, empfiehlt sich zum Beispiel ein konkreter Katalog mit Verhaltensregeln. Ebenso sollten Schulungen und Audits durch entsprechende 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 wichtiger 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 Entscheider-Ebene verankert werden muss.

Weitere Informationen: www.ceyoniq.com

Über Carsten Maßloff: *Carsten Maßloff ist Geschäftsführer und Experte für Informationssicherheit bei dem Bielefelder Software-Hersteller Ceyoniq Technology GmbH.*

Über die Ceyoniq Technology GmbH:

Seit mehr als 25 Jahren ist die Ceyoniq Technology GmbH Hersteller branchenübergreifender, intelligenter Softwarelösungen in den Bereichen DMS, ECM & EIM auf Basis der Informationsplattform nscale. Mithilfe dieser modularen, skalierbaren und hochflexiblen Informationsplattform können komplexe Geschäfts- und Kommunikationsprozesse optimiert, Daten zu werthaltigen Informationen aufgewertet und Dokumente revisionssicher und beweiskräftig archiviert werden. Hinzu kommt ein umfassendes Consulting-Portfolio für Informationssicherheit, Datenschutz und Prozessberatung der Versorgungs- und Versicherungswirtschaft. Die Ceyoniq Technology GmbH ist ein Tochterunternehmen der KYOCERA Document Solutions Inc. und beschäftigt am Hauptsitz in Bielefeld sowie an weiteren bundesweiten Standorten mehr als 150 Mitarbeiter.

Kontakt für Journalisten & Redaktionen:

Malte Limbrock
Sputnik GmbH
Presse- und Öffentlichkeitsarbeit
Lessingstraße 60
53113 Bonn
Tel.: +49 (0)228 / 30412-630
Fax: +49 (0)228 / 30412-639
limbrock@sputnik-agentur.de
www.sputnik-agentur.de

Eva Respondek
Ceyoniq Technology GmbH
Content Marketing & PR Managerin
Boulevard 9
33613 Bielefeld
Tel.: +49 (0)521 9318-1611
Fax: +49 (0)521 9318-1111
M.: +49 171 9788150
e.respondek@ceyoniq.com
www.ceyoniq.com