Homo Carens Securitate

Der Mensch, der den Mangel an Sicherheit leidet: Vom Homo Oeconomicus zum Weird Human

Sebastian Klipper
CycleSEC GmbH
Email: sk@cyclesec.com

Abstract: Unser modernes Menschenbild geht insbesondere in der Berufswelt von verantwortungsbewusst handelnden Menschen aus. Aufgrund von Überlegungen kommen diese innerhalb der Organisationen, in denen Sie beschäftigt sind zu folgerichtigen Entscheidungen. Diese Sichtweise manifestiert sich in den Wirtschaftswissenschaften in der Figur des Homo Oeconomicus – eines vorausschauenden, reaktionsschnellen Nutzenmaximierers. Auch wenn die Anwendung des Modells vom Homo Oeconomicus in den Wirtschaftswissenschaften gute Dienste leistet: In der Informationssicherheit wird es Tag für Tag widerlegt. Hier agiert der Homo Carens Securitate – als potentielles Opfer. Er trifft seine Entscheidungen auf Grundlage von hoher Risikobereitschaft bis hin zur Gefährdung des eigenen Gewinns und des Gewinns anderer, mangelhafter oder fehlender Voraussicht und einer Reaktionsfähigkeit, die weit unter der Reaktionsfähigkeit von Hackern, Crackern und Bot-Nets liegt. Vom Social Engineer wird er zum Weird Human umprogrammiert [4][5] und zu Handlungen oder Unterlassungen veranlasst, die in seiner Beschreibung als Homo Oeconomicus nicht vorgesehen sind.

I. Homo Oeconomicus

Jeder Wirtschaftswissenschaftler hat das Modell des Homo Oeconomicus im Laufe seiner Ausbildung kennen gelernt. Mit ihm werden alle möglichen Aspekte menschlichen Handelns innerhalb von Organisationen analysiert. Der Homo Oeconomicus trifft seine Entscheidungen auf Grundlage von

⇒ Maximierung des eigenen Gewinns,

⇒ vollkommener Voraussicht und

⇒ unendlich schneller Reaktionsfähigkeit.

Ein Homo Oeconomicus hat es zudem nur mit Partnern zu tun, die über die gleichen Fähigkeiten verfügen [1].

Das Model des Homo Oeconomicus geht also u.a. von konstruktiv gestaltenden Marktteilnehmern aus, die sich an eine gewisse Ordnung halten. Auch wenn die Maximierung des eigenen Nutzens im Vordergrund steht, ist ein mittel- oder unmittelbarer Schaden bei den anderen Marktteilnehmern nicht gewollt oder zumindest ethisch nicht vertretbar.

II. Homo Carens Securitate

In der Informationssicherheit haben wir es allerdings neben den „normalen“ Mitbewerbern (Konkurrenz) auch mit destruktiv gestaltenden Marktteilnehmern zu tun. Deren Gestaltungswille stellt die eigene Nutzenmaximierung über alles und nimmt dabei mittel- oder unmittelbarer Schaden bei den anderen Marktteilnehmern in Kauf oder versucht sogar, diesen gezielt zu verursachen.

In diesem Umfeld ist der Mensch ein angreifbares Wesen, dessen Vertrauen und Gutgläubigkeit von Angreifern ausgenutzt wird.

Der Homo Carens Securitate[1] trifft seine Entscheidungen auf Grundlage von...

⇒ hoher Risikobereitschaft bis hin zur Gefährdung des eigenen Gewinns und des Gewinns anderer,

⇒ mangelhafter oder fehlender Voraussicht und

⇒ einer Reaktionsfähigkeit, die weit unter der Reaktionsfähigkeit von Hackern, Crackern und Bot-Nets liegt.

III. Social Engineering

Aus diesem Blickwinkel steht der Faktor Mensch in der Informationssicherheit auf der einen Seite und der Social Engineer auf der anderen. Während der Mensch als Homo Carens Securitate einen Mangel an Sicherheit leidet und seine Entscheidungsfindung auf hoher Risikobereitschaft, mangelhafter oder fehlender Voraussicht und einer unzureichenden Reaktionsfähigkeit beruht, trumpft der Social Engineer unbeschwert auf: Aus seinem Methodenkoffer zur Ausnutzung menschlicher Schwächen wählt er das richtige Werkzeug, um Informationen zu beschaffen. Man bezeichnet diese Methoden als Social Engineering.

Social Engineering umfasst alle gewaltlosen Methoden zur Ausnutzung menschlicher Schwächen mit dem Ziel der Manipulation zu bestimmten Handlungen und der Beschaffung von Informationen. Diese ermöglichen es ihm, durch Insiderwissen eine falsche Identität vorzutäuschen oder unberechtigten Zugang zu Informationen oder IT-Systemen zu erlangen.

[1] Der Mensch der den Mangel an Sicherheit leidet

IV. Weird Human

Eine Weird Machine ist ein Computerprogramm, in dem zusätzlicher Code ausgeführt werden kann, was so in der ursprünglichen Anforderungsbeschreibung oder Spezifikation nicht vorgesehen war [3]. Dieses Modell lässt sich als Weird Human auch auf den Menschen übertragen [4]. Demnach ist ein Weird Human ein Mensch, der als Homo Carens Securitate zu Handlungen oder Unterlassungen veranlasst werden kann, die so in seiner Beschreibung als Homo Oeconomicus nicht vorgesehen waren. Durch den Missbrauch wird der Homo Carens Securitate zum Weird Human.

Ein Social Engineer vernachlässigt die Anforderungsbeschreibung an den Homo Oeconomicus und befasst sich lieber mit den praktischen Unzulänglichkeiten des Homo Carens Securitate. Sein Ziel ist es einen „Weird Human“ zu erzeugen, der beliebig missbraucht werden kann.

V. Schlussfolgerung

Während ein Social Engineer nur wenige Menschen überlisten muss, müssen Sicherheitsexperten alle potentiellen Opfer erreichen und sie vor möglichen Gefahren warnen. Es sieht aus wie ein verlorener Kampf. Wenn man ihn nur mit technischen Sicherheitsmaßnahmen, Verboten und Geboten in Sicherheitsrichtlinien gewinnen will, dann ist er das auch.

Social Engineering stellt den Homo Carens Securitate in den Mittelpunkt, während sich die Informationssicherheit häufig an den Homo Oeconomicus richtet, was der Grund für das Scheitern vieler Maßnahmen ist.

Bei der Gestaltung von Sicherheitsrichtlinien müssen wir stets von fehlerbehafteten Menschen ausgehen, die nicht mit vollkommener Voraussicht ausgestattet sind und die nicht mit unendlich schneller Reaktionsfähigkeit ihren Gewinn maximieren. Ganz im Gegenteil: Einige Menschen öffnen selbst kurz nach dem Awareness-Training und gegen besseres Wissen PDF-Dateien in Emailanhängen, auch wenn Sie dadurch substantielle Schäden für ihre Organisation verursachen. Dass die Reaktionsfähigkeit von Ermittlungsbehörden in der internationalen Zusammenarbeit auch nicht die beste ist, fällt dann kaum mehr ins Gewicht.

In der Informationssicherheit haben wir es mit einer Gattung des Menschen zu tun, der einen Mangel an Sicherheit leidet – den Homo Carens Securitate als Gegenentwurf zum Homo Oeconomicus. Unsere Aufgabe ist es zu verhindern, dass der Homo Carens Securitate zum Weird Human wird.

VI. Ausblick

Wenn man den Faktor Mensch in der Informationssicherheit aus seiner Opferrolle befreien will, muss man ein allgemeines Bewusstsein für Informationssicherheit schaffen. Zusätzlich ist die Kommunikation zu verbessern und mittelfristig eine robuste Sicherheitskultur zu etablieren.

Literatur

[1] Günter Wöhe, Einführung in die Allgemeine Betriebswirtschaftslehre, Vahlen, 19. Auflage, München 1996

[2] Sebastian Klipper, Konfliktmanagement für Sicherheitsprofis (Edition <kes>), Springer Vieweg, 2. Auflage, Wiesbaden 2015

[3] Sergey Bratus e.a., Exploit Programming From Buffer Overflows to “Weird Machines” and Theory of Computation, 2011, abrufbar unter: http://langsec.org/papers/Bratus.pdf (zuletzt abgerufen: 23.10.2016)

[4] Sebastian Klipper, Marietta Spangenberg, Der Faktor Mensch in der Informationssicherheit, Kurseinheit EIS04 der Wilhelm Büchner Hochschule, Darmstadt 2017

Anhang

A. *Über den Verfasser*

Sebastian Klipper ist Geschäftsführer und Mitgründer der CycleSEC GmbH. Er ist Autor von fünf Fachbüchern, darunter „Konfliktmanagement für Sicherheitsprofis“ [2] und Entwickler mehrerer Security-Awareness Tools. An der Wilhelm Büchner Hochschule ist er Autor der Kurseinheit „Faktor Mensch in der Informationssicherheit“ [4].

B. *Über CycleSEC*

Die CycleSEC GmbH ist ein Spin-off der Fachhochschule Münster. Die CycleSEC GmbH mit Sitz in Münster bietet anbieter- und produktneutrale Beratung und Dienstleistungen rund um die Themen Informationssicherheit, IT-Sicherheit und Cyber-Security. CycleSEC möchte die Verbindung aus Forschung und unternehmerischem Handeln im Bereich der IT-Sicherheit in NRW weiter nach vorne bringen.