IT Defense: Awareness zwischen System Spock und System Homer

Human OS

Jörg Riether

Wenn IT-affine Menschen beim Thema Awareness mit Aussagen wie „You can't patch stupid" (Du kannst Dummheit nicht flicken) argumentieren, dann sollten sie lieber einmal selbst in den Spiegel schauen. Mit diesen Worten eröffnete Lance Spitzner von SANS Security Awareness seine Keynote bei der IT Defense, die Anfang Februar in Bonn stattfand.

Menschen sind die primäre Herausforderung in der heutigen Zeit, sagt Awareness-Experte Lance Spitzner. Man könne noch so viele technische Innovationen vorantreiben – sobald ein Mensch die Tastatur auch nur anfasst, seien alle technischen Bemühungen nachrangig und die Situation gestalte sich zuweilen unberechenbar. Es wäre aber vermessen und falsch, hier die Schuld dem Nutzer zuzuweisen, vielmehr müsse man als Awareness-Verantwortlicher lernen, die Denkweise von Menschen – quasi das „menschliche Betriebssystem" – zu verstehen.

Schnelles Denken, langsames Denken

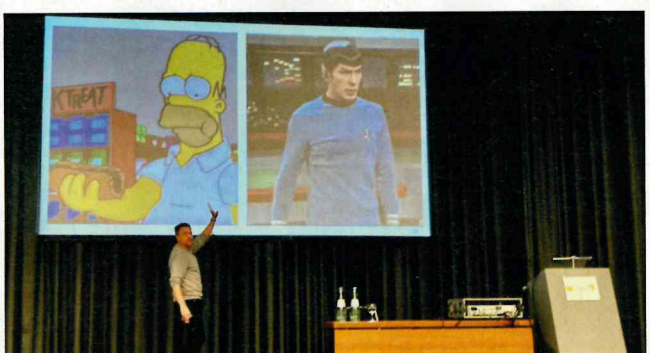
Menschen ändern sich in ihrer grundsätzlichen Denkweise nie, so sein Zwischenfazit. Er zog Parallelen zum bekannten Bestseller „Thinking, Fast and Slow" von Daniel Kahneman. Wenn man etwaige Awareness-Programme oder sonstige wichtige Sicherheitsinformationen verbreitet, sogar Informationen über aktuelle Patches und Schwachstellen, dann würden IT-Verantwortliche, Hersteller und Unternehmen immer noch in die falsche Richtung denken. Man gehe davon aus, alle Informationen würden vom „System 2" (laut Wikipedia langsam, anstrengend, selten aktiv, logisch, berechnend, bewusst) aufgenommen oder, bildlich gesprochen, von einem Mr. Spock, so Spitzners Metapher.

In Wahrheit sei es aber immer „System 1" (laut Wikipedia schnell, automatisch, immer aktiv, emotional, stereotypisierend, unbewusst), das aktiv wird – in seinem Bild Homer Simpson. Unterm Strich müsse es um Motivation und Kompetenz gehen, so Spitzner. Der Schlüssel zur Motivation sei im Kern zunächst die Betrachtung des „Warum", erst danach des „Wie" und dann erst des „Was". Man sollte ergo den Menschen mündig behandeln, ernst nehmen und zunächst einmal erläutern, warum eigentlich etwas so und nicht anders gemacht werden soll. Das eigentliche Problem müsse erklärt werden, bevor man auch nur ansatzweise irgendwelche Regeln erwähnen sollte.

Die Realität sehe aber leider so aus, dass man es viel zu oft genau andersherum macht. Aber selbst wenn man mit dem „Warum?" beginnt, dürfe man niemals vergessen, dass man zunächst mit Homer Simpson spricht. Insofern müsse man stets Emotionen ansprechen und vor allem mit Vereinfachungen arbeiten. Andernfalls sei jedwede echte Aufnahme der Awareness-spezifischen Informationen schlicht nicht möglich.

Der Schlüssel zur Befähigung sei die Vereinfachung. Was für einen selbst vollkommen nachvollziehbar und logisch erscheint, so Spitzner, muss für andere Menschen nicht so sein. Dummerweise werde dies aber fast immer vergessen. Dabei sei es so einfach – Vereinfachung könne in einem Maße helfen, wie man es sich kaum vorstellen kann. Man solle einmal darüber nachdenken, warum zuweilen kleine aufgedruckte Fliegen in Urinalen zu finden seien und warum durch diese winzige und auf den ersten Blick dümmliche Maßnahme erheblich weniger Spritzer danebengingen. Man müsse endlich den Fokus auf den Menschen richten, und zwar in erster Linie mittels Vereinfachung.

Als Negativbeispiel führte Spitzner Passwortrichtlinien vieler Unternehmen und Behörden an, etwa Regeln in Bezug auf Komplexität, Änderungszyklen, eigene Passwörter für jeden Account und bloß niemals etwas aufschreiben. Wenn man hier nicht durch Simplifizierung einschreite, so Spitzner, seien die Sicherheitsprobleme vorbestimmt. Am konkreten Beispiel könne man massiv vereinfachen, indem man Passwortabläufe abschafft, alle Richtlinien durch Technik ersetzt (etwa MFA, SSO, Biometrie), Passphrasen empfiehlt sowie die Benutzung von Passwort-Managern aktiv fördert und fordert.



Zwei Sinnbilder für zwei Denkweisen – Lance Spitzner mag anschauliche Beispiele.

Seinen eigenen Erfahrungen nach sei es viel einfacher, ein Unternehmen anzugreifen, wenn man im Vorfeld wisse, dass es dort eine Passwortänderungsrichtlinie gebe. Man könne immer davon ausgehen, dass extrem unsichere und allzu menschliche Methoden mit einer trivial definierten Abfolge von Buchstaben oder Zahlen gewählt werden. Niemals würden sich Menschen bei einer zwanghaften Änderungsrichtlinie jedes Mal ein komplexes und einzigartiges Passwort ausdenken. Dies sei einfach nicht die menschliche Natur und wenn man dies nicht endlich begreife, brauche man erst gar nicht mit weiteren Überlegungen der Verbesserung anzufangen.

Der Mensch als Sensor

Man solle außerdem, so Spitzner, ein „menschliches Sensor-Netzwerk" erzeugen. Wenn man Menschen dazu bringen könnte, aufmerksam zu sein und ihr Netzwerk über Anomalien zu benachrichtigen, dann habe man mehr gewonnen, als man mit jeder Technik erreichen könne. Dabei sei es völlig unerheblich, ob es sich um Endbenutzer, Administrationspersonal oder Entwickler handele, alles gehöre zusammen und alles wirke zusammen. Sehr hilfreich könne es zudem sein, eine Person aus der Abteilung Marketing/Unternehmenskommunikation fest in das IT-Awareness-Team zu integrieren, um ganz gezielt und kontinuierlich den Faktor Mensch anzusprechen.

Der sehr emotionale Vortrag wurde allgemein, auch im Nachgang, sehr gelobt. Spitzner schloss mit einem bekannten Zitat von Bruce Schneier: „If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology." (Wenn du glaubst, dass Technik deine Sicherheitsprobleme lösen kann, dann verstehst du die Probleme nicht und du verstehst die Technik nicht.) (ur@ix.de)