

Awareness ist Einstellungssache

Interview Tom Köhler, Microsoft

Elmar Török, bits+bites

Tom Köhler leitet bei Microsoft die Abteilung Sicherheitsstrategie und Kommunikation. Er war maßgeblich für die Durchführung einer Awareness-Kampagne verantwortlich, mit der die Microsoft-Mitarbeiter für die Gefahren des Social Engineering sensibilisiert werden sollten. Wir sprachen mit Tom Köhler über die Rahmenbedingungen für eine Awareness-Maßnahme.

IT-Grundschutz: Herr Köhler, Awareness ist in der IT-Sicherheit nicht unumstritten. Wo würden Sie diese Maßnahme in die Gesamtumgebung, bestehend aus Technik, Prozessen und Faktor Mensch einordnen?

Köhler: In den meisten Unternehmen geht es bei IT-Sicherheit in erster Linie um die technischen Maßnahmen. Das ist auch in Ordnung, doch darf man nicht vergessen, dass ein Angreifer immer nach der schwächsten Stelle suchen wird. Wenn die Firewall undurchdringlich ist, wird er sich nicht weiter damit aufhalten sondern sich ein einfacheres Ziel suchen. Nicht umsonst heißt es, dass es unwichtig ist, wie teuer die Firewall war, interessant ist nur wie teuer es wird, den Administrator zu manipulieren.

IT-Grundschutz: So ein Versuch über die Hintertür an Firmeninterne zu kommen, wird vermutlich nicht plump mit einem Umschlag voller Geld erfolgen. Wie weckt man in Mitarbeiter Aufmerksamkeit für soziale Angriffstechniken?

Köhler: Wie viel Awareness man in Firmen erzeugen muss, hängt ganz von Art und Reifegrad des Unternehmens ab. Wer täglich mit sensiblen Informationen oder Produkten arbeitet, fängt auf einem höheren Level an. Wichtig ist es, Betroffenheit in den Mitarbeitern zu wecken,

das geht nur über reale Situationen, die im täglichen Arbeitsablauf verankert sind.

IT-Grundschutz: Sie sprechen die Praxisnähe an. Nun hört man oft, dass die Awareness-Kampagnen nichts mit der Realität zu tun hätten, die Szenarien wären konstruiert und wirklichkeitsfern.

Köhler: Ich bin mir hundertprozentig sicher, dass Unternehmen heute mit genau diesen Angriffen rechnen müssen, die in den Awareness-Kampagnen durchgespielt werden. Wenn wenig über echte Vorfälle zu hören ist, liegt das vor allem an der hohen Dunkelziffer. Ich schätze, dass Industriespionagevorfälle in den Unternehmen weit über die immer wieder zitierten 20% hinausgehen.

IT-Grundschutz: Also passen die Angriffe zur echten Bedrohungslage?

Köhler: Es kommt natürlich auch auf den Dienstleister an, der die Angriffe durchführt, sprich wie gut er das Umfeld des Kunden versteht. Kann er sich gut in das Umfeld hineinendenken dann sind auch die Angriffe authentisch. Außerdem liegt es natürlich am Unternehmen selbst, die Ziele einer solchen Kampagne und damit auch die Umsetzung zu definieren. Ich würde



Tom Köhler, Direktor Strategie Informationssicherheit & Kommunikation, Microsoft Deutschland GmbH

jedem raten, erste eine Risikoanalyse durchzuführen, um die Ansatzpunkte zu finden und danach auch die Kampagne auszurichten.

IT-Grundschutz: Können Sie mir ein Beispiel nennen?

Köhler: In unserem Fall ging es ganz klar um den Bereich Großkundenbetreuer. Wie gehen sie mit Daten um, wie verhalten sie sich? Der Dienstleister muss also die Prozesse verstehen, um passende Angriffe durchzuführen. Natürlich kann es auch Sinn machen, zunächst zu klären, wo es Risiken gibt. Ein Unternehmen wie die Bundesbank hat so hohe physikalische

Zugangssperren, dass man Dinge wie Tailgating, also das Hineinschlüpfen in das Gebäude mit anderen Mitarbeitern, eher vernachlässigen kann.

IT-Grundschutz: Wie sieht die Situation im Idealfall nach einer solchen Awareness-Kampagne aus? Wie wird Erfolg oder Misserfolg bewertet?

Köhler: Um den Erfolg messen zu können, müssen vorher Ziele definiert worden sein, Sie sehen, ohne Risikoanalyse geht es nicht. In manchen Bereichen lässt sich trotzdem keine Metrik anwenden, bei anderen hingegen schon. So hat sich bei uns die Nachfrage und Nutzung der Verschlüsselungslösung als Folge der Kampagne BitLocker enorm erhöht. Das ging bis zu dem Punkt, an dem der Support die Anfragen durch die Nutzer nicht mehr hinterher kam. Und eine punktuelle Messung am Tag X nach der Kampagne ist ohnehin zu wenig. Die Aufmerksamkeit lässt nach, man muss solche Maßnahmen immer wieder durchführen.

IT-Grundschutz: Stellt sich dann nicht ein Abstumpfungseffekt ein?

Köhler: Natürlich darf man nicht die gleiche Kampagne unverändert wiederholen, da gähnen die Leute ganz schnell. Man muss sich immer wieder etwas Neues einfallen lassen um den Spannungsbogen hoch zu halten und die Aufmerksamkeit zu gewinnen. Ein paar Poster an den Wänden reichen da nicht. Das war auch der Unterschied bei Microsoft: hier haben wir zum Teil virale Effekte hervorgerufen, mit denen wir bei der Planung nie gerechnet hatten. Die Leute haben Sportsgeist entwickelt und sich richtig in das Thema reingehängt. So wurde eine von uns ins Netz gestellte Phishing-Seite schnell enttarnt, die Consultants haben nachgeforscht, den Hoster identifiziert und nach 30 Minuten eine Rundmail mit der Warnung vor der Seite verschickt.

IT-Grundschutz: Herr Köhler, wie findet ein Unternehmen, dass eine Awareness-Kampagne plant, den passenden Partner?

Köhler: Da gibt es unterschiedliche Ansätze. Ich kann nur empfehlen, auf die bisherige Erfahrung des Dienstleisters zu achten. Man sollte nur Firmen in Betracht ziehen, die schon mehrere ähnliche Projekte in ähnlichen Firmen durchgeführt

haben. Meiner Ansicht nach lohnt es sich nicht, solches Wissen erst mit dem eigenen Projekt aufzubauen. Wir haben wirklich extrem vom Erfahrungsschatz unseres Partners profitiert. Außerdem ist es wichtig auf Zertifizierungen und Qualifikationen der Mitarbeiter zu achten. Der Dienstleister gewinnt sehr detaillierte Einblicke in das eigene Unternehmen und müssen daher absolut vertrauenswürdig sein.

IT-Grundschutz: Gibt es noch etwas, das Sie potenziellen Kampagnen-Kandidaten auf den Weg geben wollen?

Köhler: Es gibt ja dieses Zitat von Kevin Mitnick, das bei Sicherheitsvorfällen mit dem Faktor Mensch immer wieder genannt wird: „Gegen Dummheit gibt es keinen Patch“. Das mag stimmen, aber wenn Dummheit nur mangelndes Wissen ist, gibt es den Patch sehr wohl in Form von Wissensvermittlung. Ich kann meine Mitarbeiter nicht für Probleme verantwortlich machen, wenn ich ihnen vorher nicht geholfen habe, die Probleme überhaupt zu erkennen.

IT-Grundschutz: Herr Köhler, wir danken Ihnen für dieses Gespräch.

Hier abonnieren

Diese Leser profitieren vom Informationsdienst IT-Grundschutz

- IT-Leiter
- Administratoren
- Sicherheitsbeauftragte
- Bezieher der IT-Grundschutzkataloge
- Datenschutzbeauftragte
- IT-Security-Officer zum schnellen Überblick und zur Weitergabe an Geschäftsleitung, IT-Leitung oder Administratoren.
- Für die Sicherheits-Verantwortlichen in Behörden und mittelständischen Unternehmen, in denen es keinen speziellen IT-Security-Officer gibt



IT-Grundschutz

Der Informationsdienst „IT-Grundschutz“ ist eine ideale aktuelle Ergänzung zu den IT-Grundschutz-Katalogen. Der monatlich erscheinende Informationsdienst liefert Neues zu Rechtsprechung, Technik, Anwendungen und Trend-Themen - leicht verständlich und praxisnah.

gratis: Probeseiten und News unter: www.grundschutz.info

Jahresabonnement Informationsdienst IT-Grundschutz:
Inland 98,00 € / Ausland 116,10 € inkl. MwSt. und Versandkosten

SecuMedia
Der Verlag für
Sicherheits-Informationen

SecuMedia Verlag
Postfach 12 34, 55205 Ingelheim
vertrieb@secumedia.de
Tel. +49 6725 9304-0