Social Engineering im militärischen Kontext

Organisationen wie die Schweizer Armee müssen ständig damit rechnen, Ziel einer so genannten Social Engineering Attacke zu werden. Potenzielle Angreifer machen sich dabei die Schwachstelle Mensch gezielt zunutze und versuchen, Mitarbeiter mit bestimmten Beeinflussungstechniken dazu zu bringen, schützenswerte Informationen zu teilen.

Mathias Schreier, Peter Stöckli, Hubert Annen

Cyber- und Datensicherheit stellt Organisationen vor grosse Herausforderungen. Während die Informatikforschung umfangreiches Wissen zu technischen Aspekten der Cyber-Sicherheit generiert, wird den Humanfaktoren noch zu wenig Beachtung geschenkt[1]. Gerade die Schwachstelle Mensch wird aber von potenziellen Angreifern gezielt genutzt. So werden Beeinflussungstechniken eingesetzt, um bei Menschen bestimmte Verhaltensweisen wie zum Beispiel die Preisgabe sensibler Informationen zu provozieren[2]. Organisationen wie die Schweizer Armee, die über besonders schützenswerte Informationen verfügen, müssen sich somit möglichst gezielt auf Social Engineering Attacken vorbereiten, indem potenzielle Angriffstechniken antizipiert und idealerweise in entsprechenden Schulungen thematisiert werden.

Überzeugungstechniken

Die sozialwissenschaftliche Forschung zu Social Engineering Attacken benennt verschiedene Überzeugungstechniken, mit denen die Angreifer an die Informationen zu gelangen versuchen[3]. Dazu gehören vor allem die von Cialdini[4] identifizierten Techniken wie beispielsweise das Knappheits-, das Konsistenz- und das Autoritätsprinzip.

Die Knappheit zielt darauf ab, dass Menschen ein rares Gut stärker begehren als ein ohne Probleme verfügbares Gut[5]. Ein Social Engineering Angreifer könnte sich dieser Technik nun bedienen, indem er in einer E-Mail darauf hinweist, dass ein E-Mail-Account gelöscht wird, falls nicht innerhalb von wenigen Stunden das Passwort erneuert wird[3]. Der Link zum Passwortwechsel führt dann aber auf eine Website, die zum Zweck hat, das eigentliche Passwort des Angegriffenen in Erfahrung zu bringen. Das knappe Gut, in diesem Fall das angeblich bald nicht mehr zur Verfügung stehende E-Mail-Konto, erhöht zusammen mit dem Zeitdruck die Wahrscheinlichkeit, dass das Passwort preisgegeben wird.

Die Konsistenz bezieht sich darauf, dass Menschen grundsätzlich eine Übereinstimmung zwischen den eigenen Werten und Handlungen anstreben, das heisst, sie möchten sich entsprechend ihrer Überzeugungen verhalten[5]. Ein Social Engineering Angreifer könnte nun beispielsweise einen Mitarbeiter der Schweizer Armee telefonisch kontaktieren und nach einer kleinen, unverfänglichen Information fragen. Falls besagter Mitarbeiter diese Frage beantwortet, meldet sich der Angreifer nun wiederholt und fragt dabei immer nach sensibleren Informationen[2]. Da der Mitarbeiter die erste harmlose Frage beantwortet hatte und sich Menschen konsistent verhalten möchten, erhöht sich nun die Wahrscheinlichkeit, dass er auch die heiklen Fragen beantwortet.

Auch mit Autorität kann man Einfluss auf das Verhalten anderer ausüben. Aussagen, die von einem (vermeintlichen) Experten stammen, werden überzeugender wahrgenommen und führen somit eher dazu, dass man einer Bitte nachkommt[5].

Autorität im militärischen Kontext

Gerade das Autoritätsprinzip dürfte in einer stark hierarchisch geprägten Organisation wie der Schweizer Armee erfolgsversprechend sein. Um folglich der Frage auf den Grund zu gehen, ob militärische Grade von potenziellen Angreifern genutzt werden könnten, wurde mit 202 Rekruten ein sozialpsychologisches Experiment durchgeführt[6]. Die Rekruten wurden dabei in die Situation eines Wachtdienstes versetzt, wo sie einen Telefonanruf erhalten, der ihnen als Audio-Datei vorgespielt wurde. Per Zufall drei verschiedenen Experimentalgruppen zugewiesen, hörten sie eine in Bezug auf das Autoritätsprinzip leicht variierte Audio-Datei. Die Datei wurde in einem Tonstudio professionell aufgenommen und so verändert, dass sie sich ausschliesslich in Bezug auf den militärischen Grad des Anrufers unterscheidet (der Wortlaut findet sich im Kasten unten).

Unmittelbar nach dem Anhören des Anrufs mussten sie angeben, mit welcher Wahrscheinlichkeit sie dem Anrufer die gewünschten Informationen (Liste der aktuell auf der Wache eingeteilten AdA) preisgeben würden. Dabei fanden sich statistisch signifikante Unterschiede zwischen den drei Gruppen: Der Anrufer,

Experiment zum Autoritätsprinzip

202 Rekruten wurden in drei verschiedene Gruppen eingeteilt und hörten den folgenden Anruf (die Unterschiede zwischen den Gruppen sind kursiv dargestellt).

«Guten Tag, hier spricht *Carl Meyer / Wachtmeister Meyer / Oberst im Generalstab Meyer*. Ich rufe an, weil wir von verschiedenen Rekrutenschulen gehört haben, dass es teilweise Probleme mit der Wache gibt. Ich bin gerade dabei, Informationen zusammenzutragen, um dieses Problem zu lösen. Aus diesem Grund brauche ich dringend folgende Information: Ich brauche eine aktuelle Liste von denjenigen Personen, die sich aktuell bei Ihnen auf der Wache befinden.»

Die Rekruten zeigten beim Anrufer, der sich als Oberst i Gst ausgab, eine höhere Bereitschaft zur Informationspreisgabe als die Rekruten in den anderen beiden Gruppen.

der sich als Oberst i Gst ausgab, erhielt die Informationen eher als der Anrufer, der sich als Wachtmeister vorstellte beziehungsweise der gar keinen Grad nannte. Die (Grad-)Autorität erhöhte also die Wahrscheinlichkeit, an sensible Informationen zu gelangen. Im vorliegenden Fall ist noch zu beachten, dass nahezu alle Rekruten zum Zeitpunkt des Experiments bereits einmal auf der Wache eingeteilt waren. Sie waren also diesbezüglich geschult und wussten, dass solche Daten nicht herausgegeben werden dürfen. Dennoch führte das blosse Nennen eines hohen militärischen Ranges zu einer erhöhten Bereitschaft, dem Anrufer die gewünschten Informationen zu übermitteln.

Auf den ersten Blick wirken diese Resultate ernüchternd. Es ist aber auch festzuhalten, dass die Wahrscheinlichkeit, die Informationen herauszurücken, generell als klein eingeschätzt wurde. Die betreffende Schulung blieb also nicht ohne Wirkung. Aber eben, in Bezug auf die wahrgenommene Autorität konnte ein Effekt nachgewiesen werden. Wenn auch nur eine Person sich von einem vermeintlichen hohen Grad beeindrucken lässt, kann das schädliche Folgen haben.

Kritisch hinterfragt werden kann auch die methodische Vorgehensweise: Die Rekruten mussten sich lediglich vorstellen, auf der Wache zu sein. Man könnte entsprechend argumentieren, dass die Resultate in der Realität anders aussehen würden. Allerdings gibt es in der sozialwissenschaftlichen Forschung diverse Hinweise, dass Ergebnisse solcher Studien mit den Ergebnissen der Realität korrelieren. Die hier angewandte Methode ist also verlässlich genug, um Ursache-Wirkungs-Beziehungen zu untersuchen[7].

Individuelle Einflussfaktoren

Nebst den oben diskutierten Überzeugungstechniken beschäftigt sich die Forschung mit weiteren Techniken[8] und Einflussfaktoren. Unter anderem weisen die Befunde darauf hin, dass jüngere Personen (18- bis 25-Jährige) anfälliger sind für Social Engineering Attacken als ältere Personen[9]. Erklärt wird dies einerseits damit, dass die betreffende Altersgruppe (noch) über einen tieferen Ausbildungsstand, über weniger Jahre an Erfahrung mit dem Internet und über weniger Zugang zu Schulungsmaterial über Phishing verfügt. Andererseits geht man davon aus, dass besagte Alterskohorte weniger risikovermeidend ist und sich deshalb eher dazu verleiten lässt, auf einen Link zu klicken und sensible Informationen einzugeben[9]. Angesichts der Tatsache, dass Rekruten genau in diese Alterskohorte fallen, ergibt es durchaus Sinn, mittels Schulungen noch stärker für diese Problematik zu sensibilisieren.

«Social Engineering umfasst den Einsatz von Manipulation, Beeinflussung und Täuschung, um eine Person innerhalb einer Organisation dazu zu bringen, einer Aufforderung nachzukommen.»

Nebst dem Alter spielt auch die Persönlichkeit eine Rolle. So sind extravierte Personen, die über eine entsprechend hohe Ausprägung in Geselligkeit, Aktivität und Gesprächigkeit[10] verfügen, sowie verträgliche Menschen, die sich durch eine hohe Ausprägung an Hilfs- und Vertrauensbereitschaft, Kooperation und Nachgiebigkeit auszeichnen[10], tendenziell anfälliger auf Social Engineering Attacken[11, 12].

Bewusstsein für Social Engineering schärfen

Insgesamt wird deutlich, dass die Erfolgswahrscheinlichkeit allfälliger Angriffe nicht nur durch die Gewandtheit der Angreifer und die Überzeugungskraft derer Techniken bedingt ist, sondern auch durch die Dispositionen der angegriffenen Person selbst. Das bedeutet, dass niemand mit absoluter Sicherheit immun gegenüber Social Engineering Angriffen ist und es sich deshalb lohnt, im Rahmen gezielter Trainingsprogramme den Fokus nicht nur auf potenzielle Methoden der Angreifer, sondern auch auf psychologische Voraussetzungen und Mechanismen in der Zielgruppe zu richten. ■

Literatur

1 Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J. (2021). Organizational science and cybersecurity: Abundant opportunities for research at the interface. Journal of Business and Psychology.

2 Bullée, J-W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2017). On the anatomy of social engineering attacks – A literature-based dissection of succesful attacks. Journal of Investigative Psychology and Offender Profiling, 15, 20–45.

3 Lawson, P., Pearson, C. J., Crowson, A., & Mayhorn, C. B. (2020). Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy. Applied Ergonomics, 86, 103084.

4 Cialdini, R. B. (1987). Influence (Vol. 3). A. Michel.

5 Goldstein, N. J., Martin, S. J., & Cialdini, R. B. (2017). YES! 60 Secrets from the science of persuasion. Profile Books Ltd.

6 Schreier, M. (2020). «Social engineering» im militärischen Kontext. ETH Zurich: unpublished bachelor thesis.

7 Siehe z. B. Rost, K., & Arnold, N. (2017). Die Vignettenanalyse in den Sozialwissenschaften – Eine anwendungsorientierte Einführung. München: Rainer Hamp Verlag.

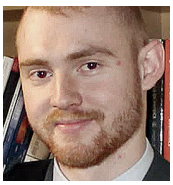
8 Siehe z. B. Ferreira, A., & Teles, S. (2019). Persuasion: How phishing emails can influence users and bypass security measures. International Journal of Human-Computer Studies, 125, 19–31.

9 Sheng, S., Lanyon, M. B., Kumaraguru, P., Crano. L., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, pp. 373–382.

10 Rammstedt, B., Kemper, C. J., Klein, M. C., Beierlein, C., & Kovaleva, A. (2013). Eine kurze Skala zur Messung der fünf Dimensionen der Persönlichkeit. Methoden, Daten, Analysen, 7, 233–249.

11 Uebelacker, S., & Quiel, S. (2014). The social engineering personality framework. In: 2014 Workshop on Socio-Tehnical Aspects in Security and Trust, IEEE, 24–30.

12 Welk, A. K., Hong, K. W., Zielinska, O. A., Tembe, R., Murphy-Hill, E., & Mayhorn, C. B. (2015). Will the «phiser-men» reel you in?: assessing individual differences in a phising detection task. Internatinoal Journal of Cyber Behavior, Psychology and Learning, 5, 1–17.



Oberleutnant
Mathias Schreier
BA ETH in public policy
Einh Kdt
4565 Recherswil

Peter Stöckli
Dr. phil.
Wissenschaftlicher Mitarbeiter
MILAK / ETH Zürich
4410 Liestal

Oberst
Hubert Annen
Dr. phil., Dozent Militärpsychologie und Militärpädagogik, MILAK/ETHZ
6300 Zug