Virtuelle Räuber, falsche Präsidenten und echte Erpresser

Carsten Hesse

Riskworkers GmbH
c.hesse@riskworkers.com

Zusammenfassung

IT-Angriffe gegen Unternehmen, Behörden und Privatpersonen haben in ihrer Quantität und Qualität ein problematisches Ausmaß erreicht. Um private und Geschäftsdaten zu stehlen, Firmen mittels Ransomware zu erpressen, oder durch „falsche Präsidenten“ virtuell zu berauben, verbinden Hacker Schadsoftware mit psychologischen Manipulationstechniken, dem sogenannten *Social Engineering*. Dabei werden mittlerweile primär jene Mitarbeiter gezielt kontaktiert und beeinflusst, die Zugang zu sensiblen Informationen haben oder relevante Geschäftsprozesse verantworten. Abwehren lassen sich diese Angriffe allein dadurch, dass zeitgemäße IT-Sicherheitslösungen mit dezidierten Schulungsmaßnahmen verknüpft werden. Letzterer, als *Awareness* bezeichneter Ansatz der Bewusstseinsbildung dient der Aufklärung und Sensibilisierung von Mitarbeitern bzw. Endanwendern gegenüber Risiken, die durch IT-Angriffe bedingt sind. Für eine langfristige Wirksamkeit und Verhaltensänderung bei den Adressaten sollte Awareness einige Prämissen erfüllen. Schulungen sollten einerseits auf tatsächliche Risiken des betreffenden Unternehmens zugeschnitten und andererseits zielgruppenspezifisch an den Mitarbeiter orientiert sein. Sinnvoll ist ein Ansatz, bei dem verschiedene methodische Bausteine, die zur Motivationssteigerung diverse Informations- & Wahrnehmungskanäle ansprechen, miteinander kombiniert und kontinuierlich angewandt werden.

1 Darstellung aktueller Risikoszenarien

Die Zahl der gegen Konzerne, Behörden und Institutionen gerichteten IT-Angriffe hat in den letzten Jahren signifikant zugenommen [ShKo16]. Neben ihrer Quantität hat auch Komplexität ein kritisches Maß erreicht; davon betroffene Unternehmen erlitten hohe Einbußen [Fren17]. Geschäftsprozesse wurden durch Hacker-Angriffe teilweise vollständig unterbunden, wichtige Akteure handlungsunfähig [Kasp16, Syma17].

Dieser Trend wird sich weiter fortsetzen [Tren17]. Der Angriff mit der Ransomware *WannaCry*, von dem weltweit nach Schätzung rund 250.000 Systeme betroffen waren, belegt diese Annahme [Alla17, Secu17, ScWI17].

Folgend werden drei Szenarien skizziert, die durch ihre Ausführungsart und die hohe Zahl betroffener Anwender besondere Aufmerksamkeit erlangt haben.

P. Schartner · A. Baumann (Hrsg.) · D•A•CH Security 2017 · syssec (2017) 259-268.

1.1 Massive Ransomware-Kampagnen

Am 13.05.2017 sahen Reisende in einigen Bahnhöfen verwundert auf Anzeigetafeln der Deutschen Bahn AG. Über den eigentlichen Zuginformationen wurde ein Pop-up-Fenster geöffnet. Zu sehen war die Mitteilung: ***„Oops, your files have been encrypted!“***. Die Reisenden wurden Zeugen des bis dahin größten koordinierten Angriffs mit so genannter *Ransomware*.

Bei solchen Kampagnen erhält in der Regel eine große Zahl von Endanwendern Mails, die im Anhang ein Tool zur Verschlüsselung von Daten enthalten. Wird dieses (unwillentlich) geöffnet, installiert sich ein Kryptographie-Programm, das Anwenderdateien mit einem starken Algorithmus verschlüsselt. Die Angreifer fordern zur Entschlüsselung Lösegeld. Die Betroffenen werden aufgefordert, Geldbeträge in einer virtuellen Währung, meist *Bitcoin*, auf ein anonymisiertes Konto zu überweisen.

Der Angriff mit der Malware *WannaCry* war kritisch, da hier eine Softwarelücke mit der Bezeichnung MS17-010 von Windows SMB (Server Message Block / Protokoll zur Dateifreigabe in Netzwerken) bei älteren Versionen des Windows-Systems, primär Windows XP & Windows 7, ausgenutzt wurde. Nach Installation hat die Malware autonom alle über ein Netzwerk bzw. Intranet mit dem Ausgangssystem verbundenen Rechner infiltriert und chiffrierte selbstständig auch darauf Anwenderdateien [Křou17].

Bei diesem und ähnlich gelagerten Szenarien wurden durch mehr oder weniger zeitgleiche Verschlüsselung einer großen Zahl von Anwendersystemen Geschäftsprozesse erheblich beeinträchtigt, teilweise komplett unterbunden. Die betroffenen Institutionen wurden handlungsunfähig. In manchen Fällen wurde das Lösegeld gezahlt [Bilf17, FuHe16, Kann16].

1.2 Advanced Persistent Threat (APT)

Fallbeispiel: Rainer Müller arbeitet in der Abteilung Corporate Communications eines internationalen Konzerns. Ihm obliegen Kontakte zu Medienvertretern. Er ist für die Außendarstellung des Unternehmens zuständig. Müller erhält irgendwann eine Mail, die vorgeblich von einem Journalisten einer Regionalzeitung stammt. Dieser teilt mit, dass er über ein Video verfüge, das einen Mitarbeiter aus Müllers Haus bei Handlungen mit einer Prostituierten in einem Hotel zeigt. Die Frau sei erkennbar minderjährig. Weiterhin liegt dem Journalisten die Hotelrechnung vor, die von Müllers Unternehmen bezahlt sei. Die Mail enthält einen Link, auf dem das Video eingesehen werden kann.

Da er für die Außenwirkung seines Hauses verantwortlich ist, muss er der Mitteilung nachgehen. Er öffnet die Video-Seite und sieht eine explizite Szene. Das Video ist grobkörnig, die Handelnden aber identifizierbar. Müller sendet über den internen Hausserver eine Mail an einen Kollegen aus der Personalabteilung mit dem Link, der Bitte um Ansicht und ggf. Identifizierung des Mitarbeiters. Von dort wird der Link noch weiter im Unternehmen geteilt. Bei jeder Ansicht des Videos wird über eine Schwachstelle im Windows-System die Malware *PlugX*, ein Remote Access Trojaner, auf dem jeweiligen Client-System installiert [OnHw14].

Der Fall verdeutlicht das Vorgehen bei komplexen Angriffen, so genannten *Advanced Persistent Threats* (APT). Ausgangspunkt ist oftmals eine Spear-Phishing-Mail, die an zuvor identifizierte Mitarbeiter gerichtet wird. Die Mail wirkt authentisch und entspricht inhaltlich dem originären Tätigkeitsfeld der Zielperson. Bei einem APT werden z.T. nur wenige Mitarbeiter

kontaktiert. Handelt es sich um Führungskräfte mit hoher Sicherheitsfreigabe, reicht die Kompromittierung eines einzelnen Systems aus. Der Trojaner öffnet auf dem Zielsystem eine „Hintertür". Darüber wird eine Verbindung zu einem Command-and-Control-Server etabliert. Die Angreifer erhalten Zugriff auf das Zielsystem, Zugangscodes und Passwörter. Damit weisen sie sich erweiterte Nutzer- bzw. Administratorrechte zu und übernehmen die vollständige Kontrolle des Rechners. Vom kompromittierten System ausgehend infiltrieren sie durch vertikale und horizontale Lateralisierung das gesamte Firmennetzwerk [GovC16]. Je nach Zielsetzung werden dann sensible Daten gestohlen oder geschäftskritische Abläufe manipuliert.

Bei „virtuellen" Banküberfällen suchen Hacker nach Systemen mit denen Geldinstitute bestimmte Prozesse realisieren [Syma16]. Dazu zählen die Auslösung von Auslandsüberweisungen, das Management von Kreditportfolios und die Wartung von Geldautomaten. Die Angreifer übernehmen deren Kontrolle und verändern diese Vorgänge zu ihren Gunsten.

In 2016 erregte der Diebstahl von $ 81 Mio. aus der Zentralbank von Bangladesch unter Nutzung des Finanzkonsortiums SWIFT weltweites Aufsehen [PeCo16]. Eine vergleichbare Beute wird den Gruppen *Carbanak* und *Metel* zugeschrieben. Weltweit sollen diese eine Vielzahl von Banken virtuell ausgeraubt haben [Grea16].

1.3 Überweisungen von „falschen" Präsidenten

Verstärkt seit dem Jahr 2013 werden Unternehmen weltweit zunehmend mit einer eigentlich alten Betrugsmasche konfrontiert; einer Variante des *Enkel-Tricks* [ProP16]: Vorgeblich leitende Manager oder Geschäftsführer kontaktieren per Telefon und scheinbar authentischen Mails Mitarbeiter, die befugt sind, Finanztransaktionen durchzuführen. Der Manager gibt vor, deren Unterstützung bei einem sensiblen Geschäft zu benötigen. Für ein Joint Venture müssen z.B. Gelder ins Ausland überwiesen oder Anteile einer Zulieferfirma erworben werden. Um das Vorhaben nicht zu gefährden, muss die Transaktion geheim bleiben. Der Mitarbeiter wird zum Stillschweigen verpflichtet, weitere Kontakte auf ein absolutes Minimum beschränkt. Alle weiteren Instruktionen zur Transaktion werden dann nur noch über externe Mailanbieter oder eine dritte Partei, z.B. eine Anwaltskanzlei übermittelt.

Unter bestimmten Voraussetzungen ist diese Betrugsmasche, die unter den Namen CEO Fraud, Fake President oder auch Business Email Compromise (BEC) bekannt wurde, extrem erfolgreich. Ein Automotive-Konzern verlor so in 2016 rund 40 Millionen Euro. Der Geschäftsführer eines Auslandsstandortes erhielt fingierte Mails, in denen er aufgefordert wurde, Geschäftsgelder auf ein anderes als das übliche Referenzkonto zu überweisen. Die Nachrichten stammten vorgeblich von der deutschen Zentrale und erschienen legitim [FAZ16].

Nach Erhebung des Bundeskriminalamtes verloren Unternehmen in Deutschland durch CEO Fraud seit 2013 rund 110 Millionen Euro [BKA16]. Weltweit beläuft sich der Schaden gemäß des US-amerikanischen FBI mittlerweile auf $ 5,3 Milliarden [FBI17].

Die Mails, auf denen BEC beruht, werden in der Regel nicht von IT-Sicherheitslösungen erkannt. Sie enthalten allein Text und keine Anhänge bzw. Links zu Malware mit spezifischer Signatur, die von Anti-Viren-Software identifizierbar wäre. BEC funktioniert allein auf Basis einer Beeinflussung.

2 Social Engineering als Bestandteil von Angriffen

Die zuvor genannten Szenarien haben eine Gemeinsamkeit: Ihr Ausgangspunkt ist eine psychologische Manipulation. Anwender werden dazu verleitet, mit Ransomware oder Spionage-Tools infizierte Email-Anhänge zu öffnen bzw. zu installieren oder eine von einem vorgeblichen Geschäftsführer autorisierte Auslandsüberweisung durchzuführen.

Diese Art des Vorgehens wird heute unter dem Begriff *Social Engineering* (SE) summiert. SE ist zum essentiellen Bestandteil moderner IT-Angriffsszenarien geworden. Kaum ein Hacker verzichtet auf diesen scheinbar immer effizienten *Modus Operandi* der Manipulation von Endanwendern, um sich Zugang zu einem technisch gesicherten System zu verschaffen.

Im Sinne einer Arbeitshypothese wird SE als Methode definiert, um jemanden gezielt dahingehend zu manipulieren, eine Handlung zu initiieren, die seiner individuellen Einstellung nicht entspricht.

Es gibt nicht die „eine“ SE-Methode. Die konkrete Umsetzung ist von der Zielsetzung und der anvisierten Zielgruppe abhängig. Mittlerweile werden primär jene Mitarbeiter gesucht und manipuliert, die tatsächlich Zugang zu sensiblen Daten haben oder geschäftskritische Prozesse verantworten. Mit Informationen, die diese Zielpersonen im Internet bzw. auf den Plattformen der sozialen Netzwerke hinterlassen, erstellen Angreifer detaillierte Profile um Ansatzpunkte z.B. für Spear-Phishing-Mails zu finden.

2.1 Wirkungsfaktoren des Social Engineering

Die Basis von SE ist die Ausnutzung grundlegender menschlicher Annahmen und Motivstrukturen. Unter anderen zählen dazu:

- Sympathie und Hilfsbereitschaft gegenüber Menschen, die uns ähnlich sind bzw. unserer „Peer-Group“ angehören
- Anerkennung und Steigerung des Selbstwertgefühls
- Die Tendenz, Komplexität, Zeit und Aufwand bei Routinetätigkeiten zu reduzieren
- Angst vor negativen Folgen des eigenen Verhaltens
- Gier und Neugier

2.1.1 Warum funktioniert SE so gut?

Die aufgeführten Motive sind Ausdruck menschlichen Verhaltens und Erlebens. Bei SE werden grundlegende Einstellungen und Annahmen ausgenutzt. Diese sind für eine funktionierende, zwischenmenschliche Interaktion essentiell und können nicht einfach „abgeschaltet“ werden. Würden sie ständig in Frage gestellt, wäre das Ausdruck einer problematischen Beeinträchtigung. Menschen, die überall nur Gefahren und böse Absichten antizipieren, werden nicht unbedingt als angenehme Zeitgenossen betrachtet.

3 Angriffsabwehr durch Awareness & IT-Lösungen

Die oben geschilderten Angriffe lassen sich lassen sich allein durch eine Kombination zeitgemäßer IT-Sicherheitslösungen mit Schulungsmaßnahmen zur Sensibilisierung und Aufklärung von Mitarbeitern abwehren.

Beide Ansätze sollten aufeinander abgestimmt sein. Es nützt z.B. wenig, wenn in einer Schulung auf Risiken hingewiesen wird, die von auf Office-Anwendungen basierenden Makroviren ausgehen, sich dann diese Makros ohne softwaregestützten Warnhinweis auf Client-Systemen öffnen lassen.

Ebenso sollten sensible Informationen nicht auf Servern gespeichert werden, auf die alle Anwender Zugriff haben. Essentiell bei der technischen Sicherung sind Prinzipien der Server-Separierung und einer mehrfaktoriellen Authentifizierung bei Zugriff auf Dateien und Prozesse.

Es ist nicht zielführend, eine Art der Standard-Aufklärung nach dem Gießkannenprinzip über allen Mitarbeitern unterschiedslos „auszugießen“. Um wirksam zu sein, sollten Sensibilisierungs- und Schulungsmaßnahmen bestimmte Prämissen erfüllen.

Von Vorteil ist, dass Awareness-Maßnahmen mit geringem Aufwand realisiert werden können. Verglichen mit Ausgaben für IT-Sicherheitslösungen und vor allem mit jenen, die zur Kompensation (erfolgreicher) Ransomware-Attacken notwendig werden, bleiben die für eine Bewusstseinsbildung der Mitarbeiter aufzuwendenden Kosten überschaubar.

3.1 Risikobegrenzung durch mehrfaktorielle Autorisierung

Generell ist es angebracht, geschäftskritische Prozesse mit einer mehrfaktoriellen Authentifizierung abzusichern. Überschreiten Finanztransaktionen einen kritischen Grenzwert oder bei Transfers auf neue, nicht vorab klar verifizierte Konten, sollte eine Prüfung durch einen weiteren Mitarbeiter bzw. Vorgesetzten erfolgen.

Gemäß dem Vier-Augen-Prinzips wird eine Überweisung erst freigegeben, wenn das System durch mindestens eine weitere Person zusätzliche Authentifizierungsmerkmale erhält. Die Autorisierungen sind dabei strikt voneinander zu trennen: Mitarbeiter A kennt das Authentifizierungsmerkmal von Mitarbeiter B nicht und hat keinen Zugriff darauf, genau wie umgekehrt.

Eine zusätzliche Authentifizierung ist auch sinnvoll, um geschäftskritische Daten oder Prozesse vor einem APT zu schützen. Auch hier bedarf dann der Zugriff auf bestimmte Daten oder die Veränderung von IT-Prozessen der Autorisierung durch mindestens einen weiteren Mitarbeiter mittels einer zusätzlichen Verifizierung.

4 Faktoren wirksamer Awareness

4.1 Risiko- und zielgruppenorientierter Ansatz

Awareness sollte auf die für das Unternehmen vordringlichen Risiken und spezifischen Mitarbeitergruppen ausgerichtet sein. Dies gilt auch für den Kosten-Nutzen-Aspekt.

Hier gilt: Wer alles und jeden schützen will, schützt niemanden.

4.1.1 Beispiele für einen risikobasierten Ansatz

Ein Unternehmen aus der Dienstleistungsbranche wird eher selten mit einem komplexen Advanced Persistent Threat mit dem Ziel eines Informationsdiebstahls konfrontiert. Fallen dafür durch einen Angriff viele Systeme gleichzeitig aus, resultiert daraus schnell Handlungsunfähigkeit. In dieser Branche besteht ein höheres Risiko für eine Ransomware-Attacke.

Da Dienstleistungsunternehmen stetigen Personalbedarf haben, bietet sich die Einschleusung von Malware mittels Online-Bewerbungen an. Entsprechend sollten Mitarbeiter im Bereich Bewerbermanagement besonders hinsichtlich Spear-Phishing-Mails sensibilisiert sein.

Beim CEO Fraud werden allein Personen manipuliert, die Finanztransaktionen verantworten, bei virtuellen Überfällen Bankangestellte mit weitreichenden Kontobefugnissen. Diese Mitarbeitergruppen sollten in Bezug auf die SE-Techniken bei APT und BCE aufgeklärt werden.

4.1.2 Risikominimierung durch zielgruppenorientierten Ansatz

Um Schadsoftware in Mails zu „verstecken", bieten sich Office-Formate wie Excel, Word oder PowerPoint an. Die Dateiformate werden von bestimmten Mitarbeitergruppen häufiger, von anderen seltener genutzt. Zu Ersteren zählen Angehörige der Abteilungen Einkauf, Controlling oder Personal. Zur Risikominimierung sollten diese Mitarbeiter spezifisch für die Identifizierung von Spear-Phishing-Angriffen sensibilisiert werden.

Mitarbeiter mit hohen Sicherheitsfreigaben wie IT-Administratoren, Führungskräfte oder Assistenten der Geschäftsleitung unterliegen einem erhöhten Angriffsrisiko. Es handelt sich um Zielpersonen für komplexe Angriffe wie APT. Werden deren Systeme kompromittiert, erhalten die Angreifer weitreichenden Zugriff auf sensible Daten und Prozesse.

Für diesen Personenkreis werden maßgeschneiderte SE-Techniken zumeist im Rahmen persönlicher Gespräche bzw. Telefonate angewandt. Diese potenziellen Zielpersonen sollten durch individuelle Briefings auf Kontaktanbahnungen durch Angreifer informiert und entsprechend vorbereitet werden.

4.2 Verpackung von Awareness & Motivierung

Im Zusammenhang mit Cyber-Angriffen und speziell SE werden Anwender manchmal etwas herablassend als DAU, *Dümmste Anzunehmende User,* bezeichnet, die sich nur allzu leichtfertig beeinflussen lassen. Weniger prekär wird das Konzept der *Schwachstelle* bzw. des Einfallstors *Mensch* herangezogen, das Hacker ausnutzen um ohne Widerstand in ein durch technische Lösungen gesichertes System einzudringen.

Für Awareness-Maßnahmen sind solche Bezeichnungen kontraproduktiv. Ein erfahrener Manager, der Opfer einer individuell geplanten, speziell gegen ihn gerichteten SE-Kampagne wurde, wird sich nur ungern als „Tölpel" bezeichnen lassen. Konfrontiert mit diesen Attributen werden Adressaten Awareness-Maßnahmen nicht besonders ernst nehmen.

Im Unternehmensalltag sind Mitarbeiter gehalten, eine Vielzahl von Informationsangeboten und interne Schulungen mit einem großen Themenspektrum wahrzunehmen. Überdruss und Demotivation können die Folge sein. So kann die Teilnahme an einer weiteren Schulung schnell als lästige Pflicht erlebt werden. Es gilt, diese schnell hinter sich zu bringen. Ein Lerneffekt ist dann nicht zu erwarten.

Um diesen Effekten entgegen zu wirken, sollte zu Beginn einer Awareness-Maßnahme immer der persönliche Nutzen für die Mitarbeiter herausgestellt werden.

Das Bewusstsein für die Risiken von IT-Angriffen hilft den Mitarbeitern nicht nur im beruflichen, sondern vor allem auch im privaten Kontext. Sie lernen, wie sie sich - und vor allem ihre Angehörigen – vor Spear-Phishing-Mails, dem Diebstahl von Bankdaten bzw. privaten Informationen oder Betrugsversuchen per Telefon (Enkel-Trick) schützen und somit eine persönliche Schädigung abwenden.

4.3 Medialer Ansatz

Zur Steigerung des Lerneffektes, um ein nachhaltiges Ergebnis und eine langfristige Verhaltensänderung bei den Adressaten zu erzielen, sollten Awareness-Maßnahmen auf verschiedenen Informations- bzw. Wahrnehmungskanälen etabliert werden.

Es gibt eine Vielzahl von Angeboten zur Bewusstseinsbildung gegen Angriffe. Das Spektrum reicht von Gummibärchen-Tütchen für „saubere“ Schreibtische (Clean-Desk-Policy) über E-Learning-Module im Corporate-Design bis zu komplexen Audits, bei denen die Resilienz von Mitarbeitern gegen konkrete Angriffe im Rahmen von Simulationen per Telefon oder in realen Kontaktgesprächen überprüft wird.

Elementar für den Lerneffekt bzw. eine nachhaltige Wirkung ist die individuelle Aktivierung von Adressaten. Ein Ansatz, bei dem Mitarbeiter z. B. allein ein „Erklärvideo“ ansehen, ohne selbst in irgendeiner Weise zu handeln, ist wenig Erfolg versprechend.

Der Einsatz solcher Filme kann sinnvoll sein, um eine große Zahl von Mitarbeitern kostengünstig in das Thema einzuführen. Ein Erklärvideo ist als sinnvoller *Einzelbaustein* von Awareness zu betrachten, der in Kombination mit anderen aktivierenden Methoden eingesetzt wird. Ein weiterer Baustein ist z.B. ein regelmäßiges Briefing durch Vorgesetzte. Im direkten Kontakt und den Möglichkeiten des persönlichen Austausches bzw. von Nachfragen können die Mitarbeiter dabei über aktuelle Angriffsszenarien aufgeklärt werden.

Zur Evaluation und der Wirksamkeitsprüfung von Awareness-Maßnahmen eignen sich SE-Penetrationstests bzw. Angriffssimulationen. Mit simulierten Spear-Phishing-Mails können große Mitarbeitergruppen parallel adressiert werden. Eine anonymisierte Auswertung der Reaktionen auf die Mails ergibt Aufschluss über den Grad der Mitarbeiter-Awareness.

Möglich sind auch individualisierte Ansätze. Dabei werden Mitarbeiter in sensiblen Tätigkeitsfeldern bzw. Verantwortungsbereichen im Rahmen von Rollenspielen, Übungen und Verhaltenstrainings sensibilisiert. Diese individuelle Aktivierung dient dazu Ausspähungsversuche bei APT frühzeitig zu erkennen und abzuwehren.

4.4 Vor- und Nachteile von Awareness-Kampagnen

Die folgende Tabelle fasst die Vor- und Nachteile von unterschiedlichen Awareness-Methoden zusammen.

Tab. 1: Vor- und Nachteile von Awareness-Methoden im Überblick

Warnhinweise / Catch-Phrases auf Tassen, Postern, Stiften „Think before Click!“ – „Be aware of suspicious mails“-Newsletter	
Vorteile	Nachteile
Schnell und günstig realisierbar	Darstellung nur einfacher Inhalte
Verteilung an große Mitarbeiterzahl möglich	Lerneffekt / Nachhaltigkeit – gering
Wiederverwertbarkeit	

"Erklär"-Videos / Comics zur Sensibilisierung gegenüber IT-Angriffen und SE Bsp.: allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Mediathek/mediathek.html, asw-bundesverband.de/Startseite/, youtube.com/embed/wTGAYdwZe5o	
Vorteile	Nachteile
Günstige / kostenfreie Angebote verfügbar	Motivation: Ansicht oft verpflichtend
Darstellung auch komplexer Inhalte möglich	Keine Möglichkeit der Rückfrage
Verteilung an große Mitarbeiterzahl über Intranet	Nach Erwerb keine Möglichkeit zur Veränderung
Regelmäßige Möglichkeit der Wiederholung	Lerneffekt / Nachhaltigkeit – gering
	Keine Interaktion möglich

E-Learning Module	
Vorteile	Nachteile
Komplettangebote bereits verfügbar	Teilweise hohe Beschaffungskosten
Darstellung komplexer Inhalte möglich	Bearbeitung ist oft verpflichtend – keine eigene Motivation
Verteilung an große Mitarbeiterzahl über Intranet	Keine Möglichkeit für Rückfragen
Module können an Corporate Design und Vorgaben angepasst werden	Lerneffekt/Nachhaltigkeit – gering *ohne* Interaktion und Erfolgskontrolle
Möglichkeit der Evaluation/Erfolgskontrolle, interaktive Inhalte, Features und Abschlusstests	Mitunter Probleme mit Betriebsrat wg. potenzieller Prüfungssituation
Regelmäßige Wiederholung möglich	
Hoher Lerneffekt bei Interaktion und regelmäßiger Anwendung mit neuen Inhalten	

Seminare und Briefings	
Vorteile	Nachteile
Darstellung komplexer Inhalte möglich Realisierung zielgruppenspezifischer Inhalte	Effektiv nur bei begrenzter Teilnehmerzahl weniger als 15 Teilnehmer
Hohe Interaktion durch Übungen und Rollenspiele	Kosten- und Zeitfaktor
Abstimmung auf Unternehmenssituation möglich	
Beachtung aktueller Angriffsszenarien	
Möglichkeit der Evaluation/Erfolgskontrolle	
Hoher Lerneffekt durch Interaktion und bei regelmäßiger Wiederholung, min. einmal pro Jahr	

Angriffssimulationen/SE-Penetrationstests mit Phishing-Mails und SE-Anrufen	
Vorteile	Nachteile
Angebote sind bereits auf dem Markt verfügbar	Kostenfaktor
Tests können an Zielgruppen angepasst werden	Rechtliche Hürden und Compliance
Verbreitung an große Mitarbeiterzahl über Email	Geringer Lerneffekt bei nur einmaliger Anwendung
Möglichkeit der Evaluation/Erfolgskontrolle	
Regelmäßige Wiederholbarkeit	
Beachtung aktueller Angriffsszenarien	
Hoher Lerneffekt bei regelmäßiger Wiederholung	

„Serious Games“ – Bsp.: www.known-sense.de/de/Awareness/Games/	
Vorteile	Nachteile
Bereits auf dem Markt verfügbar	Kosten- und Zeitfaktor der Vorbereitung
Darstellung von Inhalte in Spielszenarien	Nur effektiv in Kleingruppen von 5 bis max. 10 Mitarbeiter
Hoher Interaktionsfaktor durch Spielsituation	
Motivation der Teilnehmer / hoher Lerneffekt	
Zielgruppenspezifische Inhalte	
Möglichkeit der Evaluation/Erfolgskontrolle	

Literatur

[Alla17] All About Security / ohne Autor: Technische Analyse der „WannaCry“-Ransomsoftware. https://www.all-about-security.de/security-artikel/threats-and-co/artikel/17620-technische-analyse-der-wannacry-ransomware/ (2017)

[Bilf17] D. Bilfesky: Hackers Squeeze Hotel by Locking Doors. In: New York Times v. 31.01.2017, unter: https://www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html?partner=rss&emc=rss&_r=0 (2017)

[BKA16] Bundeskriminalamt (Hrsg): Wirtschaftskriminalität. Bundeslagebild (2016) p.8.

[FAZ16] Frankfurter Allgemeine Zeitung / ohne Autor v. 16.08.2016: http://www.faz.net/aktuell/wirtschaft/unternehmen/autozulieferer-leoni-um-millionensumme-betrogen-14390918.html (2016)

[FBI17] Federal Bureau of Investigations / USA / o. Autor: Business E-mail Compromise E-Mail Account Compromise The 5 Billion Dollar Scam. In: Public Service Announcement des FBI v. 04.05.2017. www.ic3.gov/media/2017/170504.aspx

[FuHe16] B. Fuest, Th. Heuzeroth: Wie Hacker mit Lösch-Attacken Lösegeld erpressen. In: welt.de unter: http://www.welt.de/wirtschaft/webwelt/article153299828/Wie-Hacker-mit-Loesch-Attacken-Loesegeld-erpressen.html (2017)

[Fren17] S. Frenkel: Cyberattack Proving Grounds. In: New York Times v. 02.07.2017: https://www.nytimes.com/2017/07/02/technology/hackers-find-ideal-testing-ground-for-attacks-developing-countries.html

[GovC16] GovCert CH/ o. Autor: Technical Report About the RUAG Espionage Case. In: Swiss Government Computer Emergency Response Team Blog. https://www.govcert.admin.ch/blog/22/technical-report-about-the-ruag-espionage-case (2016)

[Grea16] GreAT: APT-Style Bank Robberies Increase With Metel, GCMAN and Carbanak 2.0 Attacks. In: Kaspersky Lab Securelist Blog https://securelist.com/blog/research/73638/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/ (2016)

[Kann16] A. Kannenberg: Erpressungstrojaner: Stadtverwaltung kauft sich mit 1,3 Bitcoin frei. In: heise online: http://www.heise.de/newsticker/meldung/Erpressungstrojaner-Stadtverwaltung-kauft-sich-mit-1-3-Bitcoin-frei-3128957.html (2016)

[Kasp16] Kaspersky Security Bulletin / ohne Autor: Jahresrückblick / Statistik 2016/2017. https://de.securelist.com/analysis/kaspersky-security-bulletin/72294/kaspersky-security-bulletin-2016-executive-summary/ (2016)

[Křou17] J. Křoustek: Update zu WannaCry. In Avast Blog unter: https://blog.avast.com/de/update-zu-wannacry-schlimmster-ransomware-angriff-der-geschichte? (2017)

[OnHw14] G.M. Ong, C.R. Hwa: Pacific Ring of Fire: PlugX/Kaba. In: FireEye blogs unter: https://www.fireeye.com/blog/threat-research/2014/07/pacific-ring-of-fire-plugx-kaba.html (2014)

[PeCo16] N. Perlroth, M. Corkery: North Koreans Tied to Attacks at Asian Banks. In: New York Times v. 27.05.2016. http://www.nytimes.com/2016/05/27/business/dealbook/north-korea-linked-to-digital-thefts-from-global-banks.html? https://www.nytimes.com/2016/05/14/business/dealbook/details-emerge-on-global-bank-heists-by-hackers.html? (2016)

[ProP16] Polizeiliche Kriminalprävention der Länder und des Bundes / ohne Autor unter: http://www.polizei-beratung.de/themen-und-tipps/betrug/enkeltrick/ (2016)

[ScWI17] M. Scott, N. Wingfield: Hacking Attack Has Security Experts Scrambling to Contain Fallout In: New York Times, P. A15 v. 13.05.2017 unter: https://www.nytimes.com/2017/05/13/world/asia/cyberattacks-online-security-.html?partner=rss&emc=rss (2017)

[Secu17] SecureWorks / ohne Autor: WCry Ransomware Analysis. Counter Threat Unit Research. www.secureworks.com/research/wcry-ransomware-analysis (2017)

[ShKo16] M. Shad, C. Kopke: Industrie im Visier von Cyberkriminellen und Nachrichtendiensten. In: Pressemitteilung der Bitkom e.V. https://www.bitkom.org/Presse/Presseinformation/Industrie-im-Visier-von-Cyberkriminellen-und-Nachrichtendiensten.html (2016)

[Syma16] Symantec Security Response / ohne Autor: Odinaff: New Trojan Used in High Level Financial Attacks. In: Symantec Official Blog: https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks (2016)

[Syma17] Symantec / ohne Autor: 2017 Internet Security Threat Report. Unter: https://www.symantec.com/security-center/threat-report (2017)

[Tren17] Trendmicro / ohne Autor: Die nächste Stufe. Acht Sicherheitsvorhersagen für 2017. http://www.trendmicro.de/sicherheitsinformationen/forschung/sicherheits-vorhersagen-2017/index.html (2017)