F.6

IT-Sicherheit – Unterricht

Einheit: Angriffe auf die Datensicherheit durch *Social Engineering* und *Phishing*

Redaktion RAAbits Online Informatik RAABE Verlag

In dieser Lerneinheit beschäftigt sich Ihre Klasse mit Angriffen auf sensible Daten durch *Social Engineering* und dessen Sonderform *Phishing*. Ein fiktives Beispiel eines Hackerangriffs dient als motivierender Einstieg in die Einheit. Anhand von auf zwei Niveaustufen vorliegenden Informationstexten informieren sich die Schülerinnen und Schüler über die wesentlichen Eigenschaften sowie mögliche Gegenmaßnahmen von *Social Engineering* und *Phishing*. In Aufgaben und einer Lernzielkontrolle rekapitulieren sie die thematischen Kerninhalte und werden für den kritischen Umgang mit Mails und Kontaktaufnahmen durch Fremde sensibilisiert.

KOMPETENZPROFIL DER UNTERRICHTSEINHEIT

Klassenstufe:	9–10
Dauer:	3–4 Unterrichtsstunden
Lernziele:	Die Lernenden 1. definieren *Social Engineering* und *Phishing*, 2. beschreiben Methoden des *Social Engineerings*, 3. erkennen *Phishing*-Mails an typischen Merkmalen, 4. erläutern Gegenmaßnahmen zum Schutz vor *Social-Engineering-Angriffen für Unternehmen und Privatpersonen*.
Thematische Bereiche:	Datensicherheit, *Social Engineering*, *Phishing*
Kompetenzen:	Analysieren und Reflektieren

Auf einen Blick

Einstieg

Thema:	Hackerangriff auf Daten
M 1	**Einstieg: Hacker**
M 2	**Einstieg: *Social Engineering***

Erarbeitung

Thema:	*Social Engineering und Phishing*
M 3a	**Informationstext: *Social Engineering* / M-Niveau**
M 3b	**Informationstext: *Social Engineering* / G-Niveau**
M 4a	**Informationstext: *Phishing* als Sonderform des Social Engineerings / M-Niveau**
M 4b	**Informationstext: *Phishing* als Sonderform des Social Engineerings / G-Niveau**
M 5	**Aufgaben zu *Social Engineering* und *Phishing***

Ergebnissicherung

Thema:	*Social Engineering*
M 6	**Infoblatt *Social Engineering***

Lernzielkontrolle

Thema:	*Social Engineering und Phishing*
M 7	**Lernzielkontrolle: *Social Engineering, Phishing***

Erklärung der Symbolen

	Dieses Symbol markiert differenziertes Material. Wenn nicht anders ausgewiesen, befinden sich die Materialien auf mittlerem Niveau.
	leichtes Niveau
	mittleres Niveau
	schwieriges Niveau

Informationstext: *Social Engineering*

M 3a

Was ist *Social Engineering*?

Social Engineering, auch soziale Manipulation genannt, ist das Ausnutzen menschlicher Eigenschaften und Schwächen, um an geheime Informationen zu kommen. Dies ist eine sehr effiziente Methode, um die Datensicherheit eines Unternehmens auszuhebeln.

© Pixabay

Beispiele für *Social Engineering*

Dieses Szenario ist ein typisches Beispiel: Ein gut vorbereiteter Hacker hat bereits zuvor in anderen Quellen, zum Beispiel im Internet, in Unternehmensinformationen, über Bürotratsch u. a. recherchiert, kennt die Namen der leitenden Mitarbeitenden, die Struktur etc. Dann ruft er bei einem arglosen Mitarbeitenden an und versucht, das technisch ungebildete Opfer mit Fachjargon zu verwirren oder den Autoritätsaspekt auszunutzen, indem er mit dem Chef droht. Auf diese Weise kann er bei ungeschulten Mitarbeitenden häufig sein Ziel erreichen und vertrauliche Informationen erschleichen.

Ein weiteres typisches Szenario: Ein Hacker ruft bei der Abteilung an, die für die Administration des Netzwerkes im Unternehmen zuständig ist, und behauptet, ein Mitglied des oberen Führungskreises zu sein und sein Kennwort vergessen zu haben. Selbstverständlich braucht er unmittelbar und sofort Zugriff auf seine Daten. Deshalb muss das Kennwort auf einen neuen Wert gesetzt werden, den er selbst vorgibt. Ein gut vorbereiteter Angreifer hat sich vorher schlaugemacht und weiß, wie er die jeweilige Rolle am besten spielt. Kennt er zum Beispiel den Namen des Chefs des angerufenen Mitarbeitenden, droht er glaubwürdig damit, diesen sofort anzurufen, wenn sein Wunsch nicht umgehend erfüllt wird. Dies wird für den Mitarbeitenden selbstverständlich Konsequenzen haben. Mit ein paar unfreundlichen Worten über den Chef der Abteilung verabschiedet er sich ... und hat das Spiel gewonnen und häufig Zugriff auf streng vertrauliche Daten. Das Ganze ohne irgendwelche speziellen Computerkenntnisse.

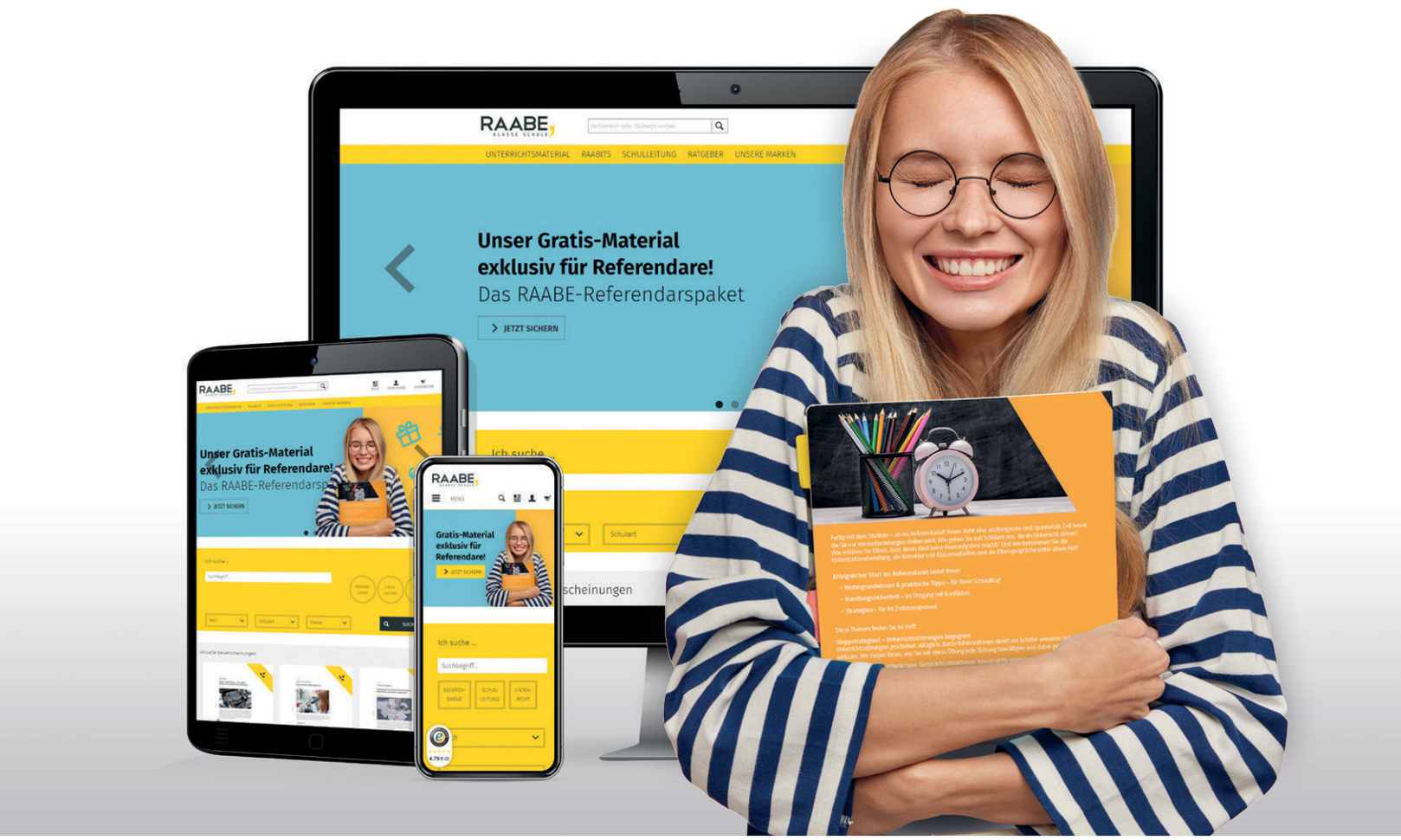
Gegenmaßnahmen

Gegen *Social Engineering* hilft nur eine genaue Festlegung von Sicherheitsrichtlinien und deren strikte Einhaltung. Angestellte müssen dahingehend geschult werden, dass sie nie Kennwörter weitergeben, auch wenn der Vorstand des Konzerns oder der Papst persönlich anrufen. Jeder verwendet und kennt grundsätzlich nur sein eigenes Kennwort. Und ein Administrator setzt ein Kennwort nur zurück, wenn er/die Mitarbeitende persönlich bei ihm erscheint oder der/die Vorgesetzte dies schriftlich anfordert. Das bedeutet aber auch, dass diese Regeln auch in ihren Konsequenzen respektiert werden müssen. Und der Chef, der einmal wirklich sein Kennwort vergessen hat, sich dann nicht aufregen darf, wenn er unter Umständen etwas warten muss, bevor er wieder an die Daten kommt – bis sich nämlich der Administrator anderweitig versichert hat, mit wem er es wirklich zu tun hat.

RAABE
KLASSE SCHULE

Sie wollen mehr für Ihr Fach?

Bekommen Sie: Ganz einfach zum Download
im RAABE Webshop.



- **Über 5.000 Unterrichtseinheiten**
  sofort zum Download verfügbar
- **Webinare und Videos**
  für Ihre fachliche und
  persönliche Weiterbildung
- **Attraktive Vergünstigungen** für Referendar:innen
  mit bis zu 15% Rabatt
- **Käuferschutz**
  mit Trusted Shops

TRUSTED SHOPS GUARANTEE

Jetzt entdecken:

www.raabe.de