Name: .....

Leseverstehen

insgesamt 90 Minuten

Aufgabe 2 | Blatt 1 10 Punkte

Situation: Lesen Sie den folgenden Text und fügen Sie die Abschnitte A – G (Blatt 2) an der richtigen Stelle (1 – 5) im Text ein. Achtung: Zwei Abschnitte passen nicht in den Text!

Der Feind in meinem Büro

Unter einem „Hacker" stellt man sich landläufig einen verschrobenen Freak vor, der einsam vor seinem Bildschirm bis spätnachts fieberhaft daran tüftelt, wie man die gut gesicherten EDV-Systeme großer Firmen oder Institutionen „knacken" könnte. Solche Exzentriker gibt es zwar – doch den größten wirtschaftlichen Schaden richtet ein anderer Täter-Typ an. Die meisten so genannten „Hackerangriffe" auf Unternehmen, so fand eine Studie unlängst heraus, werden von den eigenen Mitarbeitern ausgeführt.
Sie „sniffern" durch das Computernetzwerk der Firma und lesen die E-Mails ihrer Kollegen. Die Gehälter der Chefs kennen sie genau, und wenn sie so richtig sauer sind, legen sie auch mal den Server ihres Arbeitgebers lahm: Mehr als 60 Prozent aller Hackerangriffe auf Unternehmen kommen von den eigenen Mitarbeitern.

1 [ ]

Dabei investiert die Wirtschaft durchaus in die Sicherheit. Die Unternehmensberatung Frost & Sullivan glaubt, dass der Gesamtumsatz auf dem Markt für Datensicherheit in den nächsten Jahren von 524,6 Millionen Dollar auf 3,13 Milliarden Dollar steigen wird. Einer der stärksten Posten (43,4 Prozent) werden Produkte sein, die die Benützung von E-Mail und Internet während der Arbeitszeit überprüfen.

2 [ ]

Investitionen in solche Kontrollmaßnahmen ändern jedoch nichts daran, dass allzu oft einfachste Sicherheitsregeln missachtet werden. Viele Mitarbeiter kleben sich zum Beispiel einen Merkzettel mit ihrem Passwort direkt an den PC!

3 [ ]

Es sind ganz profane Anreize, die kriminelle Energien bei den Angestellten freisetzen. Wer seiner eigenen Firma wertvolle Daten entwendet, will dafür in der Regel Geld sehen. Aber auch Profilierungssucht, Frust oder schlicht Neugier sind Antriebsfaktoren.

4 [ ]

Gegen diese Täter aus den eigenen Reihen gibt es durchaus schlagkräftige Abwehrmethoden, wenn auch eine hundertprozentige Sicherheit unmöglich ist, wie die Berater zugeben. Doch viele Firmen versuchen nicht einmal, sich diesem Ziel anzunähern. „Meistens sorgt sich der Kunde nur nebenher um dieses Thema", weiß Bröhl aus Erfahrung.

5 [ ]

Leere Drohungen seien jedoch meist schnell enttarnt und machten wenig Eindruck – darum müssten überführte Mitarbeiter dann auch tatsächlich konsequent gekündigt und angezeigt werden.

[aus einer deutschen Zeitschrift]

Name: .....

Leseverstehen

insgesamt 90 Minuten

Aufgabe 2 | Blatt 2 10 Punkte

Situation: Lesen Sie die Abschnitte A – G und fügen Sie sie an der richtigen Stelle (1 – 5) im Text (Blatt 1) ein. Achtung: Zwei Abschnitte passen nicht in den Text!

A

„Oder sie verraten einem angeblichen Systemadministrator am Telefon arglos einen Zugangscode oder ein Passwort", erzählt Andreas Bröhl. Was aber veranlasst Angestellte zu kriminellen Taten wie z. B. Datenraub?

B

Die Medien benutzen das Wort Hacker hauptsächlich kriminalisierend, um Ängste zu schüren. Dabei sind Hacker eigentlich in der Regel ehrenhafte, zumindest aber intelligente Menschen, das Wort ist also kein Schimpfwort, sondern eine Auszeichnung, die nicht vorschnell verliehen werden sollte.

C

Doch die betroffenen Unternehmen vertuschen die meisten Fälle, meint Andreas Bröhl, Berater beim Systemintegrator Articon-Integralis. Sofern sie überhaupt etwas davon bemerken. Zwar sichere sich heute fast jedes Unternehmen über digitale Schutzwälle, so genannte Firewalls, nach außen hin ab. Dem Feind in den eigenen vier Wänden hingegen servieren sie wertvolle Daten auf dem Silbertablett.

D

Derartige Beweggründe sind wahren Hackern fremd: Diese klinken sich in fremde Computernetzwerke ein, um Sicherheitsmängel aufzudecken. Im Gegensatz zu den sogenannten „Crackern", die böswillig in der eigenen Firma hacken und klauen.

E

Er empfiehlt außerdem den Sicherheitsbeauftragten das „Anti-Hacker-Buch für Windows", das die Sicherheitsarchitektur des Betriebssystems aus dem Blickwinkel des Hackers analysiert und Verteidigungsstrategien aufzeigt.

F

Diese Programme sollen Firmenchefs die Kontrolle darüber erleichtern, wie oft ihre Angestellten nur zum Vergnügen im World Wide Web surfen oder ob der elektronische Postverkehr vornehmlich der privaten Freundschaftspflege dient.

G

Seine Einschätzung bestätigt eine Studie, laut der sogar Unternehmen, die Handel über das Internet treiben, in mehr als 40 Prozent ohne einen Sicherheitsbeauftragten arbeiten. Um Mitarbeiter vom Hacken abzuschrecken, empfehlen Experten einen „Mix aus angedrohter Strafe und Entdeckungsrisiko".