Hinweis: Bei den Lösungen handelt es sich lediglich um Lösungsvorschläge.

Prüfungssatz 6

Aufgabe 1

Teil 1

Name des Anrufers: Jonathan Miles, er ist Projektmanager
Firma: *Better Chemicals Ltd.*
Grund für den Anruf/Problembeschreibung: Um 3:36 Uhr morgens wurde ein Angriff auf das Netzwerk und auf die Server der Firma verübt; Angreifer hat die Protokolldateien gelöscht und keine verwertbaren Information zurückgelassen
Weitere Vorgehensweise: Wiederherstellung der Sicherheitsprotokolle, wenigstens teilweise, durch uns; wir sollen feststellen, welche Daten der Angreifer abgerufen hat und wie er Zugang zum Netzwerk erhielt.
Eine Mitarbeiterin, Frau Richards, wird nach München fliegen und die Festplatten mit den bereits gelöschten Protokolldateien mitbringen.
Ankunft: München 10:15 Uhr, BA 394, bitte vom Flughafen abholen

Teil 2

1. Port 80 wird für unsicheres Surfen im Internet benutzt, Port 443 für sicheres Surfen im Internet; die Ports können Verkehr zu verschiedenen Anwendungen filtern.
2. Es manipuliert den Netzwerkverkehr, der in bzw. durch den Rechner läuft, oder entscheidet, was damit passiert.
3. Iptables ist eine Datenbank von Regeln, mittels derer die Netfilter Firewall konfiguriert wird.
4. Die Benutzer öffnen und schließen TCP- und UDP 'ports'.
5. – Linux Kommandozeile: traditionelles Interface für die Konfiguration der Firewall-Regeln
   – UFW: Front-End für iptables und hostbasierte Firewalls; wurde für Ubuntu und andere Betriebssysteme entwickelt
   – Gufw: grafischer Front-End, wird für Anfänger empfohlen
   – Firestarter: grafischer Front-End in Linuxsystemen, vollfunktional; es gibt keine Updates mehr
   – Guarddog: Front-End für iptables, die mit KDEbasierten Desktops funktionieren; komplex aber flexibel

Aufgabe 2

From: (student's email address)
To: (Mr Miles's email address)
Subject: Feedback

Dear Mr Miles(,)

Mr Andres asked me to give you some feedback as soon as possible. Our team was able to at least partially recover the protocol files. Many data blocks were beyond recovery, however. An analysis with our own specialized tools is not possible. I will conduct this analysis manually and that could take some time, unfortunately. We will compile a chronological summary of the attack and hope to find answers to the following questions:

1. When did the attack begin?
2. How did the attacker gain access to the network?

KMK-Fremdsprachenzertifikat Englisch
für gewerblich-technische und IT-Berufe
ISBN: 978-3-12-800077-0

3. Was the root of the problem a security hole for which our company can be held accountable?
4. Which data were accessed?

Best regards(,)
(student's name and surname)
Assistant to Mr Andres

Aufgabe 3

- Angriff begann 02:45;
- Angreifer versuchte zwischen 02:45 und 2:49 unter verschiedenen Benutzernamen unberechtigten Zugang zu erhalten;
- für Zeitraum 02:49:03–03:01:45 keine Aufzeichnungen;
- 03:01:46 Sicherheitssystem aktiviert, da Server zu viele erfolglose Anmeldeversuche registrierte;
- Zugang zum Server für 5 Minuten gesperrt, IP-Adresse des Angreifers auf Blacklist gesetzt;
- 03:06:30 Angreifer versuchte neue Verbindung zum Server aufzubauen;
- Verbindung zurückgewiesen, da IP-Eintrag auf der Blacklist entsprach;
- 03:10:11 Angreifer baute von einer anderen IP aus neue Verbindung auf;
- zwischen 03:10:23 und 03:10:48 verschickte Angreifer fehlerhafte und unzulässige Pakete an verschiedene Anschlüsse des Servers;
- für Zeitraum 03:10:50–03:17:23 keine Aufzeichnungen;
- 03:17:49 Sicherheitssystem erneut aktiviert, da Server mögliche Exploit oder Flooding Attacke registrierte;
- Zugang zum Server für 5 Minuten gesperrt, IP-Adresse des Angreifers auf Blacklist;
- 03:22:58 Zugriff auf Webseite von Better Chemicals, Aufruf Seite über den Projektmanager Mr Miles;
- 03:35:55 Verbindung zum Server mit selbiger IP;
- nach zwei fehlgeschlagenen Anmeldeversuchen erhielt Angreifer Zugang zum Server, angemeldet als „miles" mit Passwort „jonathan1954";
- danach Zugriff auf aktuelle Projektdaten, hochgeladen per FTP auf Rechner des Angreifers;
- schließlich Herunterladen und anschließendes Ausführen eines Skripts mit Namen „cleanerscript";
- Abbruch der Protokollierung

Aufgabe 4

1. – Speicherung/Auslagerung der Daten an Orten, wo es für den Dienstanbieter am günstigsten ist.
   – Im Falle von Gerichtsverfahren hat der Betreiber die volle Kontrolle über alle Beweismittel.
2. – US Firmen lassen ihre Verträge von amerikanischen Rechtsexperten ausarbeiten.
   – Verträge lassen in der Regel wenig Spielraum für Verhandlungen und basieren auf US-amerikanischem Recht.
   – Umgang mit diesen Verträgen erfolgt durch US Richter.
3. Benutzer des Dienstes trägt das Risiko im Falle der Unterbrechung des Dienstes, bei Verlust oder Beschädigung der Daten oder bei Zugriff durch Dritte und Regierungsbehörden.
4. CVML wünscht sich die Aufnahme folgender sechs Punkte in das geltende europäische Recht zum Schutz europäischer Kunden
   – Wie in der Finanzbranche sollen gewisse Indikatoren in Bezug auf Dienstverfügbarkeit, Backup-Vorkehrungen und Preisgestaltung für Transparenz sorgen.

KMK-Fremdsprachenzertifikat Englisch
für gewerblich-technische und IT-Berufe
ISBN: 978-3-12-800077-0

- Verpflichtung der Cloud-Betreiber zur detaillierten Auskunft über schädigende Ereignisse sowie alle Maßnahmen, die getroffen wurden, um die Schäden einzugrenzen, damit der Kunde die Möglichkeit hat, alle notwendigen Maßnahmen einzuleiten, um seine Geschäftsvorgänge zu schützen.
- Problem der Daten-Rückgabe: Die meisten Verträge sind eher vage und die Situation ist nicht akzeptabel; Kunde sollte die Garantie haben, dass er die Daten bei Vertragsende in einem Standardformat erhält, das von einem anderen Dienstanbieter genutzt werden kann.
- Möglichkeit für den Kunden gemäß Punkt 4 „Kontrolle und Zertifizierung" die Überwachung der Einrichtung, die seine Daten bereitstellt; zumindest Zertifizierung der Cloud-Betreiber durch einen Dritten wie in vielen Branchen üblich
- Möglichkeit für den Endbenutzer seinen Fall vor seinem eigenen nationalen Gericht verhandeln zu lassen und der örtliche Richter sollte die Befugnis haben, wirklich effektive Rechtsmittel einsetzen zu können.
- Es geht CVML um die Durchsetzbarkeit der ersten fünf Punkte. Dazu müsste es möglich sein, dass die genannten Punkte an die Stelle widersprüchlicher Vertragsbedingungen treten und diese unwirksam werden lassen.

KMK-Fremdsprachenzertifikat Englisch
für gewerblich-technische und IT-Berufe
ISBN: 978-3-12-800077-0