württembergische
Der Fels in der Brandung.

Die Cyber-Police: Schadenbeispiele aus der Praxis

(Hinweis: Die Schadenfälle basieren auf realen Cyber-Vorfällen, zur Verdeutlichung des Schadenpotenzials)

1) DoS-Angriff: VN bietet Anlagen und Geräte aus dem Bereich Telekommunikation über typische Handelswege dem Einzel- und Großhandel an. Kleingeräte wie bspw. Handys werden auch über einen Onlineshop direkt an Endkunden verkauft. Über einen Zeitraum von 5 Tagen wurden die Server durch einen DoS-Angriff nahezu vollständig blockiert, so dass ein deutlich geringerer Warenumsatz erfolgte.

2) Diebstahl von Daten: VN entwickelt Isolationsmaterial für feuerbeständige Baugruppen wie bspw. Leichtbauwände und Feuerschutztüren. Nachts und in arbeitsfreien Zeiträumen erfolgten nachweislich Zugriffe auf Datenbestände. Offensichtlich war es Hackern gelungen die Firewall zu umgehen und auf den Server zuzugreifen. VN hat die Vermutung, dass der Angriff nicht zufällig erfolgte, da gezielt die Datenbank mit Testdaten ausgelesen wurde. Bisher ist nichts über die Nutzung der entwendeten Datenbestände bekannt geworden. Da unser VN auch im Auftrag Materialien entwickelt und prüft, mussten die Auftraggeber entsprechend informiert werden. Neben Aufwendungen für forensische Untersuchungen entstanden Kosten für Information und Kommunikation mit den Auftraggebern.

3) Hacker haben die Rechner in mehreren Hotels manipuliert. Auf den Hotel-Computern haben die Datendiebe sogenannte "Keylogger" installiert, mit denen sie Eingaben über die Tastatur mitlesen konnten. Auf diese Weise wurden Passwörter und Bankdaten gesammelt. Hoteliers wird empfohlen, öffentliche PCs so einzustellen, dass Gäste keine Administratoren-Rechte erhalten und die BIOS-Einstellungen der Rechner mit einem Passwort geschützt werden. Außerdem ist es grundsätzlich empfehlenswert öffentliche Rechner nur zum Surfen im Netz zu nutzen.

4) Bei einem kleinen Unternehmen, dessen E-Mail-Verkehr gehackt wurde, änderten die Angreifer die Bankverbindung in einer elektronisch verschickten Rechnung und lenkten so den Rechnungsbetrag auf ein anderes Konto.

5) Datenpannen bei Freiberuflern und kleineren Unternehmen
   - Gerichtsakten werden auf einer Mülldeponie gefunden. Ein Rechtsanwalt hatte sie nicht ordnungsgemäß entsorgt.
   - Auf einem Laptop, der aus dem verschlossenen Auto eines Bäckereimitarbeiters gestohlen wurde, befanden sich personenbezogene Daten aktueller und ehemaliger Mitarbeiter.
   - Ein verlorener USB-Stick eines Wirtschaftsprüfungsunternehmens enthielt vertrauliche Bilanzdaten von Kunden.

   Die Beispiele veranschaulichen die Vielzahl an Möglichkeiten, wie personenbezogene Daten gefährdet sein können. Die Verantwortung liegt bei dem Unternehmen, das personenbezogene Daten für seine Mitarbeiter oder Kunden verarbeitet oder verarbeiten lässt - egal, ob es sich dabei um das Unternehmen handelt, das die Daten auch tatsachlich verloren hat.

   Unternehmen unterliegen in Deutschland folgenden Rechtspflichten:
   - Benachrichtigung betroffener Kunden/Mitarbeiter
   - Benachrichtigung der Datenschutzaufsichtsbehörde des Bundeslandes

   Die Größe des Unternehmens spielt hierbei keine Rolle. Die Eckkneipe muss sich genauso daran halten wie Amazon. Als „sicherer Hafen“ bleibt häufig nur ein geringes Schadenrisiko und Datenverschlüsselung. Kann das Unternehmen nachweisen, dass es unwahrscheinlich ist, dass auf personenbezogene Daten zugegriffen wurde oder sie verwendet wurden, kann die Informationspflicht hinfällig werden. Bei Hardwareverlusten können zudem hohe Aufwände bei der Feststellung entstehen, welche Betroffenen im Einzelnen zu benachrichtigen sind. Zusätzlich fallen Kosten für die Aufklärung des Sachverhalts, Rechtsberatungskosten und ggfs. Haftpflichtansprüche gegen das vom Datenverlust betroffene Unternehmen an.

6) Mit einem Hacker-Angriff erbeuteten Unbekannte zahlreiche sensible Daten aus dem Server eines Konzertveranstalters. Mit den ausspionierten Bankdaten buchten die Unbekannten mehrfach Beträge von den Kreditkarten-Konten der Rock-Fans ab. Schadenersatzforderungen und Vertragsstrafen der Kreditkartenindustrie müssen beglichen werden.

Die Cyber-Police: Schadenbeispiele aus der Praxis

(Hinweis: Die Schadenfälle basieren auf realen Cyber-Vorfällen, zur Verdeutlichung des Schadenpotenzials)

7) Ein großer Einzelhändler befürchtet nach Datenklau auf Jahre Belastungen. Der Hacker-Angriff werde die Geschäfte im laufenden Quartal, in diesem Jahr und auch danach dämpfen. Kriminelle hatten die Daten von Kunden gestohlen. Kredit- und sonstige Bankkartendaten, Namen, Email- und Lieferadressen sowie Telefonnummern. Die Kriminellen verschafften sich Zugang über einen Dienstleister, der Kühlgeräte reparierte und seine Rechnungen in ein Abrechnungssystem einstellen musste. Von dort gelangten die Kriminellen in das Hauptsystem und verteilten Programme auf die Registrierkassen in den Supermärkten. Damit zeichneten die Hacker bei Einkäufen von Kunden die Kreditkartendaten, Geheimzahlen und Umsatzdaten auf. Seither bieten die Kriminellen die Kreditkartendaten in sogenannten Cardshops online an. Käufer statten Blanko-Karten mit den Daten aus oder ziehen Bargeld an Automaten.

8) Überall dort, wo sehr viele Daten erfasst werden, ergibt sich für kriminelle Hacker die Chance an verwertbare Daten zu kommen. Das gilt insbesondere für Daten bei Online-Buchungssystemen, bspw. bei einem Hotel. Wird der vorgegebene Standard der Kreditkartenindustrie nicht eingehalten, kann es hier zu empfindlichen Forderungen der Kreditkartenindustrie kommen. Und natürlich wird die Reputation eines Hauses dadurch beeinträchtigt. Und was passiert wenn das hoteleigene WLAN-Netz die Daten von Hotelgästen nicht wirksam sichert?

9) Die Webseite einer Gaststätte wird von Hackern so verändert, dass statt eines mondänen Restaurant-Bildes die Innenansicht eines in die Jahre gekommenen Fast-Food-Restaurants gezeigt wird.

10) Ein Trojaner verschlüsselt den Zugang zum IT-System eines Handwerkers. Der Sanitär-Handwerker bekommt das Angebot, die Verschlüsselung gegen Zahlung einer Geldsumme wieder aufzuheben. Die Entschlüsselung kann auf einer Webseite der Erpresser getestet werden. Sofern nicht bezahlt wird, kann die Behebung rasch einen fünfstelligen Betrag erfordern. Solche Erpressungsversuche sind sehr häufig. Nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) wurden in 2014 monatlich 2000 Erpressungsversuche (privat und gewerblich) gemeldet. (Mitversichert über die Cyber Police ist die Entschlüsselung, nicht die Lösegeldzahlung)

11) Über soziale Netzwerke werden gezielt Mitarbeiter ausgespäht, um auf Sie zugeschnittene E-Mails versenden zu können, die einen Trojaner beinhalten. Dieses „Spear Phishing“ ist eine gezielte Angriffsmethode gegen ausgesuchte Personen wie Mitarbeiter mit Administrationsrechten oder Mitglieder der Führungsebene eines Unternehmens. Es ist daher eine Sensibilisierung der Mitarbeiter hinsichtlich der Methoden des Social Engineering zu empfehlen.

12) Es geht sehr einfach: Ein 15-jähriger Hauptschüler aus Niederösterreich knackte innerhalb von drei Monaten die Computersysteme von 259 Firmen. Er stahl geheime Zugangsdaten und stellte diese ins Internet. Doch letztendlich war er nicht der geniale Hacker, der er gerne sein wollte. Mit im Internet frei erhältlichen Hacker-Tools hat der Hauptschüler die Computer-Systeme der Firmen nach Schwachstellen und Sicherheitslücken abgesucht, um dann seine Hackerangriffe durchzuführen. Unter den Firmen sind alle Branchen vertreten, von Sportfirmen über Tourismus-Dienstleister bis hin zur Erotikbranche. Die Reputation der Firmen ist angegriffen.

13) Fehlbedienung eines Mitarbeiters: Die Logistik des Warenwirtschaftssystems funktionierte deshalb nicht mehr, es konnten kaum noch Produkte ausgeliefert werden. Dadurch kam es zu hohen Umsatzeinbußen.

14) Unbekannte konnten bei einem Hackerangriff auf einen Internetoptiker auf die Kundendatenbank zugreifen. Die Angreifer hatten dabei Zugriff auf Adressdaten und Passwörter und haben diese möglicherweise auch kopiert. Zahlungsinformationen seien nicht betroffen, da diese nicht gespeichert werden. Der Betreiber hat allen Kunden jeweils ein neues Passwort per Mail zugesendet, was das Problem allerdings nicht gänzlich aus der Welt schafft. Schließlich dürften die Datendiebe mit den geklauten Passwörtern in vielen Fällen wegen Mehrfachnutzung auch auf die Mailkonten der Kunden zugreifen können. Das Unternehmen hat mittlerweile Strafanzeige gegen Unbekannt gestellt. Von dem Angriff seien Bestell- und Adressdaten von mehreren hunderttausend Kunden, aber keine Konten- oder Kreditkartendaten betroffen gewesen.

Die Cyber-Police: Schadenbeispiele aus der Praxis

(Hinweis: Die Schadenfälle basieren auf realen Cyber-Vorfällen, zur Verdeutlichung des Schadenpotenzials)

15) Ein Online-Händler, der auf die Google-Suche angewiesen ist, tauchte nicht mehr in der Google-Suche auf. In der URL-Adresse hatte ein Unbekannter pornographische Begriffe eingebaut. Damit fiel der Händler aus dem Google-Ranking.

16) Mittels einer Email installierte sich auf dem IT-System eines kleinen Maklerbüros ein Verschlüsselungstrojaner. Bis der Angriff bemerkt wurde, konnte der Trojaner schon längere Zeit aktiv sein und insbesondere die Back-ups des Unternehmens infizieren. Nach einiger Zeit ging nichts mehr: Das IT-Netz des Maklers war für mehrere Tage außer Betrieb gesetzt. IT-Dienstleister und Forensiker mussten insgesamt 17 Manntage investieren, bis die Systeme komplett gesäubert und wieder voll einsatzfähig waren. Auch wurden personenbezogene Daten ausgelesen und kursierten bereits im Netz. 150 Betroffene waren zu benachrichtigen. Die Gesamtkosten des Schadens lagen bei mehreren zehntausend Euro.

17) Auf 130 000 Euro belief sich der Schaden eines deutschen Nahrungsmittelherstellers. Hacker hatten die vollautomatisierte Produktionsstraße manipuliert und die Einstellungen zur Beigabe von Gewürzen verändert. Die betroffene Produktionscharge war unbrauchbar, erhebliche Rechercheaufwände und Kosten durch den Ertragsausfall entstanden. Die Motive der unbekannten Angreifer liegen bis heute im Dunkeln.
Mitversichert über die Cyber-Police wären die forensische Aufklärung und die Kosten des Ertragsausfalls bis zur Wiederherstellung der IT-Funktionalität.

18) Unbekannte haben den Server eines Heidelberger Sternelokals gehackt. Es wurden wahllos E-Mails an alle Kontakte verschickt, die sich auf dem Webserver befinden und jemals kontaktiert wurden. In den versendeten E-Mails wurden erfundene Zahlungsaufforderungen für vermeintlich ausstehenden Rechnungen angehängt. Die Emails gingen auch an Kunden, mit denen das Lokal gar nichts mehr zu tun hat, die teilweise auch im Ausland sind, so z.B. Griechenland, Monaco und Spanien. Es ist außerdem zu befürchten, dass sich in den E-Mail-Anhängen Viren verstecken könnten. Das Lokal wird mit Beschwerden überrollt. Es mussten automatische Telefonansagen geschalten und über die Homepage auf das Problem aufmerksam gemacht werden. Die Rückverfolgung des Angriffs dauert noch an.

19) Kriminelle Angreifer drangen in die Telefonanlage eines Mittelständlers mit 150 Beschäftigten ein. Sie fischten dort keine Daten ab, lauschten auch nicht auf der Suche nach Firmengeheimnissen - sondern sie telefonierten. Die Hacker riefen teure Nummern an, möglicherweise eigens dafür geschaltete gebührenpflichtige Dienste. Der Gesamtschaden zeigte sich auf der Telefonrechnung: 60.000 EUR hatten die Eindringlinge in wenigen Wochen vertelefoniert.

20) Die Gäste eines Restaurants und Nutzer einer Kreditkarte sind unbemerkt Opfer einer großangelegten Datenklau-Attacke geworden. Shoppingtouren in New York, die die Kreditkarteninhaber niemals tätigten, wurden von ihren Karten abgebucht. Alle Geschädigten hatten zuvor in dem Restaurant mit Kreditkarte bezahlt. Das IT-System des Restaurants war so manipuliert, dass beim Einlesen der Karten die Daten entwendet und auf neue Karten überspielt wurden. Entweder haben Hacker das Virus eingeschleust oder ein entsprechend präparierter USB Stick wurde in einem unbemerkten Moment an die Kasse angeschlossen, um das Schadprogramm aufzuspielen. Der Virus konnte trotz langwieriger Arbeiten nicht aus dem IT-System entfernt werden, die Hardware musste ausgetauscht werden.

21) Immer häufiger treten Fälle auf, bei denen Unternehmen gehackt und Original-Rechnungen von Lieferanten gesucht werden. Dabei machen sich die Hacker mit dem Schriftverkehr vertraut und versuchen den Rechnungsbetrag durch Manipulation der Original-Rechnung auf ein fremdes Konto umzuleiten. Die E-Mail-Adresse des Lieferanten wird dabei nur um ein Zeichen abgeändert, so dass der Mitarbeiter im Unternehmen das leicht übersehen kann.

Die Cyber-Police: Schadenbeispiele aus der Praxis

(Hinweis: Die Schadenfälle basieren auf realen Cyber-Vorfällen, zur Verdeutlichung des Schadenpotenzials)

22) Unbekannte hatten sich Zugang zum EDV-System eines Online-Reifenmarktes verschafft und einen Trojaner eingeschleust, der alle Daten auf dem Server verschlüsselte. Sie forderten ein Lösegeld für die Entschlüsselung. Der Unternehmer schaltete einen Computerfachmann und die Kripo ein, die dringend von der Bezahlung der Lösegeldforderung abrieten. Stattdessen musste der Trojaner entfernt und die vorhanden Datensicherungen neu aufgespielt werden. Der Betrieb stand 5 Tage still und es hat weitere 4 Tage gedauert, bis das System wieder störungsfrei arbeitsfähig war.

23) Der Verschlüsselungs-Trojaner Locky fand über einen E-Mailanhang den Weg auf die Server eines großen Autohauses und verteilte sich unbemerkt im gesamten System. Über Nacht wurden alle Daten wie Bestellungen, Abrechnungsdaten, Serviceintervalle usw. verschlüsselt. Der Betrieb stand komplett still. Auch die Datensicherungen wurden befallen, da diese mit dem Netzwerk gekoppelt waren. Die letzte nicht befallene Datensicherung war aus dem Jahr 2009, da diese vom System getrennt gelagert wurde. Das Autohaus erreichte eine Lösegeldforderung in Höhe von 30.000 EUR. Da ohne den Entschlüsselungscode kein Betrieb mehr möglich gewesen wäre und eine Rücksicherung der Daten nicht möglich war, bezahlte das Unternehmen den geforderten Betrag.