IT-Sicherheit

- Sicherheit vernetzter Systeme -

Einschub:
Verizon 2009 Data Breach Investigations (Supplemental) Report

Inhalt

- Externe Aufklärung von erkannten IT-Sicherheitsvorfällen
- Überblick über die 15 häufigsten Bedrohungen 2009
- Ausgewählte Bedrohungen
  - Angriffsmethodik
  - Erkennen von Angriffen
  - Prophylaxe

Externe Aufklärung von IT-Sicherheitsvorfällen

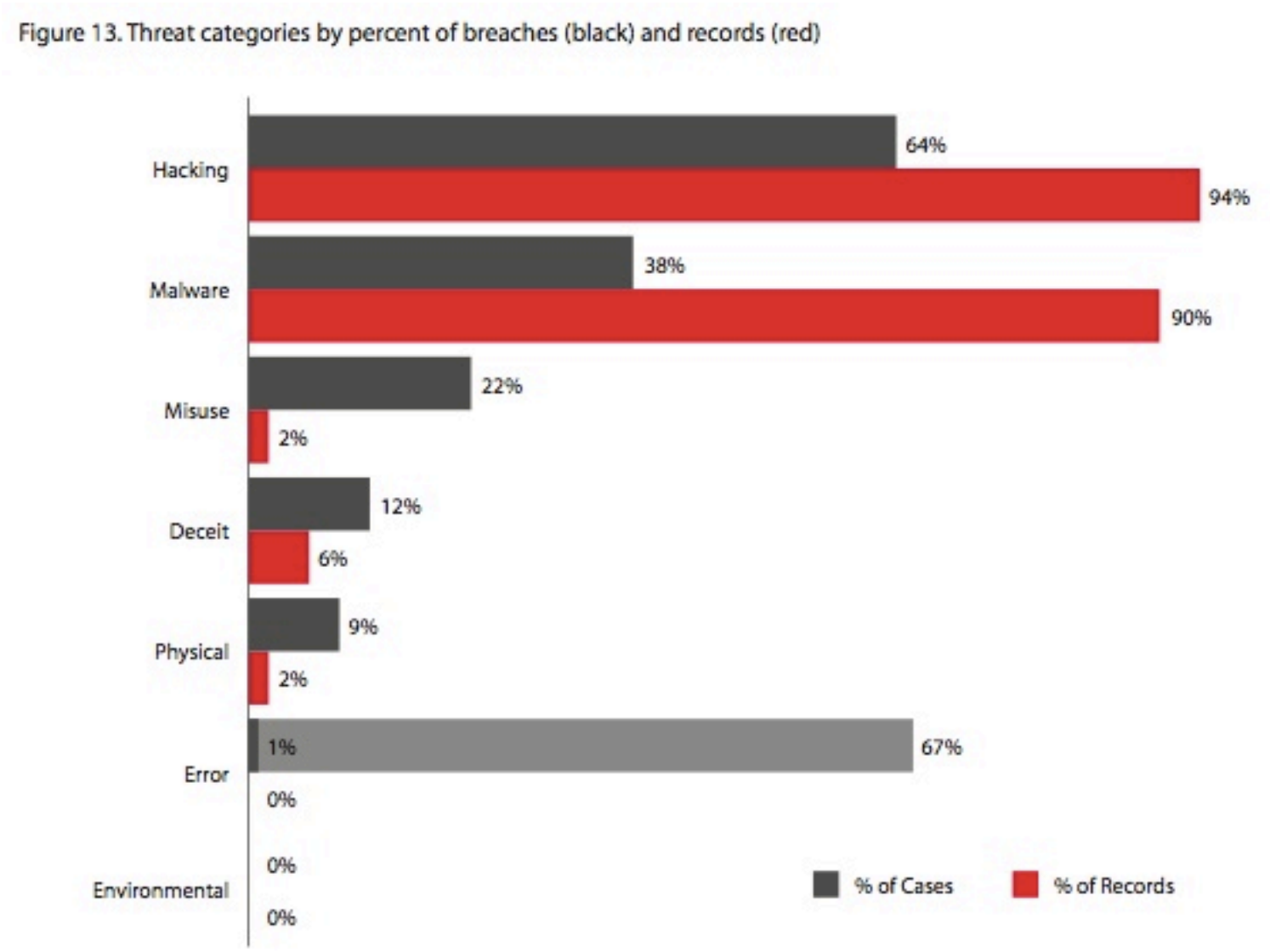
- Irgendwann wird das Problem bemerkt:
  - Systeme verhalten sich seltsam,
  - Kundendaten werden im Internet veröffentlicht,
  - Erpresser meldet sich, ...
- Vorfall muss möglichst genau aufgeklärt werden:
  - Wiederholungen verhindern
  - Juristische Aspekte (Haftung, Fahrlässigkeit, ...)
  - Sicherheit kontinuierlich verbessern
- Aufklärung häufig durch externe Dritte:
  - Oft kein firmeninternes IT-Forensik-Know-How vorhanden
  - Neutrale Analysen und Berichte als Beweismittel vor Gericht
  - Gefahr versuchter Vertuschung z.B. bei börsennotierten Unternehmen

Data Breach Report von Verizon

- Verizon Business
  - bietet IT-Forensik-Dienste für verschiedene Branchen
  - bekommt somit einen guten Überblick über erfolgreiche Einbrüche in IT-Systeme
  - fasst die Ergebnisse anonymisiert in jährlichen Berichten zusammen
- Dienstleisterberichte / White Papers sollten durchaus skeptisch betrachtet werden:
  - Behandeltes Themenspektrum nicht zwingend repräsentativ
  - Themenauswahl und -aufbereitung möglicherweise auch unter Marketing-Aspekten
  - Quellen können meist nicht überprüft werden
  - Keine externe Sicherung der fachlichen Qualität vor Veröffentlichung
- Nehmen als das, was es ist: Interessanter Überblick

Verizon Report: Überblick

- Verizon spezialisiert sich auf Angriffe, bei denen personen-bezogene Daten von externen Angreifern gestohlen wurden
- Interner Missbrauch (z.B. durch Mitarbeiter) kommt damit möglicher-weise zu kurz



Quelle: Verizon Business

Top 15 Bedrohungen lt. Verizon

Threat Category	Threat Action Type	Legend	% of Breaches	% of Records
Malware	Keyloggers and Spyware	KEYLOG	19%	82%
Malware	Backdoor or Command/Control	BACKDR	18%	79%
Hacking	SQL injection	SQLINJ	18%	79%
Misuse	Abuse of system access/privileges	ABUSE	17%	1%
Hacking	Unauthorized access via default credentials[2]	DFCRED	16%	53%
Misuse	Violation of Acceptable Use and other policies[3]	POLICY	12%	<1%
Hacking	Unauthorized access via weak or misconfigured ACLs	WKACL	10%	66%
Malware	Packet sniffer[4]	SNIFFER	9%	89%
Hacking	Unauthorized access via stolen credentials	STLCRED	8%	<1%
Deceit	Pretexting (Social Engineering)	SOCIAL	8%	2%
Hacking	Authentication bypass	BYPASS	6%	<1%
Physical	Physical theft of asset	THEFT	6%	2%
Hacking	Brute-force attack	BRUTE	4%	7%
Malware	RAM scraper[4]	RAMSCR	4%	<1%
Deceit	Phishing (and *ishing variations)	PHISH	4%	4%

Quelle: Verizon Business

Top 15 Bedrohungen (graphisch)

Quelle: Verizon Business

Bedrohung Nr. 1: Keylogger und Spyware

- Angriffsmethodik
  - U.a. Usernamen und Passwörter über Hardware, Software oder elektromagnetische / akustische Analyse abhören
  - Installation z.B. durch Benutzer (trojanisches Pferd), Lücke im Web-Browser oder bei physischem Zugang
  - Besonders häufig im Einzelhandel und in der Finanzbranche
  - Relevant in 19% der Fälle und bei 82% der gestohlenen Daten
- Erkennung durch Viren-/Malware-Scanner
  - Auffällige Prozesse laufen im Hintergrund
  - Dateien mit abgehörten Informationen im Filesystem
- Prophylaxe
  - Benutzer dürfen keine eigene Software installieren
  - Einmal-Passwörter
  - Ausgehenden Netzverkehr genau beobachten (Egress filtering)

Quelle: Verizon Business

Bedrohung Nr. 2: Backdoor or Command/Control

- Angriffsmethodik:
  - System (meist Server) wird über bekannte Sicherheitslücke kompromittiert
  - Angreifer installiert Software, um auch nach Schließen der Sicherheitslücke uneingeschränkten Systemzugang zu erhalten
  - Z.B. Austausch von Systemprogrammen und Serverdiensten (SSH, ...), Einfügen eigener Kernelmodule, ...
  - Relevant in 18% der Vorfälle und bei 79% der gestohlenen Daten
- Angriffserkennung:
  - Unerklärbare Systemaktivitäten / -last durch versteckte Hintergrundprozesse
  - Auffälliger Netzverkehr
- Prophylaxe:
  - Integritätssicherung durch Host Intrusion Detection Systeme
  - Zugriffseinschränkung durch Paketfilter-Firewalls
  - Zeitnahes Einspielen von Security-Patches für Serverdienste

Quelle: Verizon Business

Bedrohung Nr. 3: SQL Injection

- Angriffsmethodik:
  - Manipulation von Datenbankzugriffen bei mangelhafter Überprüfung der (bösartigen) Dateneingabe durch die Web-Anwendung
  - Ausmaß reicht vom Auslesen über das Manipulieren der gespeicherten Daten bis zur Kompromittierung des Datenbank-Servers
  - Relevant für 18% der Vorfälle und bei 79% der gestohlenen Daten
- Angriffserkennung:
  - Unübliche Einträge in Webserver- und Datenbank-Logfiles
- Prophylaxe:
  - Beim Implementieren auf Überprüfung von Benutzereingaben achten
  - Datenbank-Accounts mit minimal notwendigen Rechten anlegen
  - Datenbank-Fehlermeldungen nicht an Web-Client weiterleiten
  - Web Application Firewalls
  - Individuelle Penetrationstests

Quelle: Verizon Business

Bedrohung Nr. 4: Abuse of system access/privileges

- Angriffsmethodik:
  - Missbrauch der bewusst z.B. an Mitarbeiter oder Kunden/Anwender vergebenen Berechtigungen
  - besonders häufig z.B. bei gekündigten Administratoren
  - Relevant in 17% der Vorfälle, aber „nur“ bei 1% der gestohlenen Daten
  - Besonders häufig in der Finanzbranche und bei IT-Dienstleistern
- Angriffserkennung:
  - Überwachung aller privilegierten Accounts
  - Verhaltensanalyse (z.B. ungewöhnliche Login-Zeiten)
- Prophylaxe:
  - Auch administrative Accounts nur mit minimalen Rechten ausstatten
  - Separater Account pro Administrator
  - Erzwungene Protokollierung aller Eingaben (z.B. durch SSH-Daemon auf Server)
  - Rechte entziehen, bevor Missbrauch wahrscheinlicher wird (z.B. bereits vor Mitteilung der Kündigung)

Quelle: Verizon Business

Bedrohung Nr. 5: Default Credentials

- Angriffsmethodik:
  - Hard- und Softwaresysteme werden vorkonfiguriert ausgeliefert und z.B. mit den Default-Passwörtern vom Kunden in Betrieb genommen
  - Relevant in 16% der Vorfälle und bei 53% der gestohlenen Daten
  - Besonders häufig im Einzelhandel und der Lebensmittelindustrie
- Angriffserkennung:
  - Logins von unbekannten externen Adressen und/oder zu ungewöhnlichen Uhrzeiten
- Prophylaxe:
  - Keine Systeme im Auslieferungszustand in Produktivbetrieb nehmen
  - Default-Accounts löschen / Passwörter unbedingt ändern
  - Penetrationstests mit bekannten Default-Passwörtern

Quelle: Verizon Business

Bedrohung Nr. 6: Acceptable Use Policy violation

- Angriffsmethodik:
  - Mitarbeiter halten sich nicht an Einschränkungen z.B. bzgl. privater Internet-Nutzung mit Firmennotebooks
  - In der Folge Infektion mit Malware
  - Relevant in 12% der Vorfälle und bei < 1% der gestohlenen Daten
  - Häufig nicht Primärursache für Vorfälle, sondern vorbereitend oder additiv
- Angriffserkennung:
  - Auf Verstoß gegen Richtlinien prüfen (z.B. automatischer Scan von Browsercache und -history, Überprüfen von Proxy-Logfiles)
  - Virenscanner meldet Schadsoftware
- Prophylaxe:
  - Sicherheitsschulung und Sensibilisierung der Mitarbeiter
  - Benutzerrichtlinien einfach und klar verständlich halten
  - Angedrohte Sanktionen konsequent umsetzen

Quelle: Verizon Business

Bedrohung Nr. 7: Weak or misconfigured ACLs

- Angriffsmethodik:
  - Angreifer nutzt fehlende oder unzureichende Berechtigungseinschränkungen aus
  - Relevant in (nur!) 10% der Vorfälle und bei 66% der gestohlenen Datensätze
- Angriffserkennung:
  - Logfileüberprüfung
  - Verhaltensanalyse (z.B. Standort des Benutzers und Uhrzeit beim Login)
  - Intrusion Detection Systeme
- Prophylaxe:
  - Whitelist-Ansatz, d.h. alles verbieten, was nicht explizit erlaubt wurde
  - Minimale Berechtigungsvergabe an Benutzer und Administratoren
  - Zentrale Erfassung vergebener Berechtigungen

Quelle: Verizon Business

Bedrohung Nr. 8: Packet Sniffer

- Angriffsmethodik:
  - Angreifer nutzt kompromittierte Maschine oder physischen Netzzugang, um weitere Datenpakete abzuhören
  - Greift unverschlüsselte Datenpakete ab, selbst wenn Festplattenverschlüsselung genutzt wird
  - Ergebnisse werden häufig zunächst lokal gespeichert und nicht sofort per Internet übertragen
  - Relevant in 9% der Vorfälle und bei 89% der gestohlenen Daten
- Angriffserkennung:
  - Systeme mit Netzwerkkarten im „promiscuous mode“ suchen
  - Systeme mit großen Dateien / Schwankungen in der Plattenplatz-Belegung suchen
- Prophylaxe:
  - Separation des Netzdatenverkehrs
  - Verschlüsselte Datenübertragung auch im LAN
  - Host Intrusion Detection Systeme und Egress Filtering

Quelle: Verizon Business

Bedrohung Nr. 9: Stolen Credentials

- Angriffsmethodik:
  - Angreifer bringt Username/Passwort in Erfahrung oder gelangt in den Besitz von Smartcards, ...
  - „Insider“-Variante: Geschäftspartner/Kollege bestiehlt Mitarbeiter
  - Relevant in 8% der Vorfälle und bei < 1% der gestohlenen Daten
- Angriffserkennung:
  - Schwierig, da Angriff zunächst nach legitimem Zugriff aussieht
  - Logfile-Überwachung und Verhaltensanalyse
  - Anzeige der letzten Nutzungsdaten („last login“) beim Anmelden
- Prophylaxe:
  - Two-factor-authentication
  - Forcierte regelmäßige Passwortänderungen

Quelle: Verizon Business

Bedrohung Nr. 10: Social Engineering

- Angriffsmethodik:
  - Angreifer bringt Opfer dazu, sensible Informationen preiszugeben oder unscheinbare Aktionen im Rahmen eines Angriffs auszuführen
  - Vorgefunden in 8% der Vorfälle und bei 2% der gestohlenen Daten
  - Besonders häufig im Finanzwesen und bei IT-Dienstleistern - möglicherweise wegen besserer technischer Schutzmaßnahmen
- Angriffserkennung:
  - Bei guten Angriffen nur sehr schwer zeitnah zu erkennen
  - Auf ungewöhnliche Anfragen achten
- Prophylaxe:
  - Sensibilisierung der Mitarbeiter
  - Klar vorgegebene Richtlinien und Abläufe für die Auskunftserteilung
  - Ungewöhnliche Vorkommnisse melden lassen
  - Öffentlich zugängliche Informationen über Mitarbeiter auf einen sinnvollen Umfang einschränken

Quelle: Verizon Business

Bedrohung Nr. 11: Authentication bypass

- Angriffsmethodik:
  - Ausnutzung von (Software-)Fehlern, um ein System ohne Kenntnis des richtigen Passworts nutzen zu können
  - Relevant in 6% der Vorfälle und bei < 1% der gestohlenen Daten
- Angriffserkennung:
  - Logfile-Einträge auf Auffälligkeiten überprüfen
  - Intrusion Detection Systeme
- Prophylaxe:
  - Security-Aspekte bei der Software-Entwicklung von Anfang an beachten
  - Penetration Testing der eigenen Anwendungen
  - Vorgeschaltete Sicherheitsmaßnahmen, z.B. Web Application Firewalls

Quelle: Verizon Business

Bedrohung Nr. 12: Diebstahl

- Angriffsmethodik:
  - Angreifer bringt nicht nur Authentifizierungsinformationen in seinen Besitz, sondern ganze Geräte (Notebook, Smartphone, PC, ...)
  - Relevant für 6% der Vorfälle und bei 2% der gestohlenen Daten
- Angriffserkennung:
  - Fehlende Hardware
  - Videoüberwachung
  - Unbekannte Personen ohne Mitarbeiterausweis
- Prophylaxe:
  - Verschlüsselung der Daten mindestens auf mobilen Geräten
  - Datenträger vor der Verschrottung vollständig löschen
  - Ggf. Personenkontrolle am Ein-/Ausgang

Quelle: Verizon Business

Bedrohung Nr. 13: Brute-force attack

- Angriffsmethodik:
  - Z.B. Ausprobieren aller möglichen Passwörter, bis das richtige gefunden wurde
  - Besonders häufig im Einzelhandel und in der Gastronomie
  - Relevant in 4% der Vorfälle und bei 7% der gestohlenen Daten
- Angriffserkennung:
  - Logfileeinträge über gescheiterte Login-Versuche
  - Vermehrt Helpdesk-Anrufe bzgl. Freischalten automatisch gesperrter Kennungen
- Prophylaxe:
  - Passwort-Qualität über Passwort-Richtlinien sicherstellen
  - Inkrementelle Verzögerung von wiederholten Authentifizierungsversuchen desselben Benutzers
  - Two-factor-authentication

Quelle: Verizon Business

Bedrohung Nr. 14: RAM scraper

- Angriffsmethodik:
  - Schadsoftware durchsucht das RAM des befallenen Rechners nach „interessanten“ Daten
  - Dadurch Umgehung von Festplattenverschlüsselung
  - Relevant in 4% der Vorfälle und für 1% der gestohlenen Daten; Tendenz steigend
  - Bislang im Einzelhandel und in der Tourismusbranche am häufigsten
- Angriffserkennung:
  - Ähnlich wie bei anderer Schadsoftware, z.B. ungewöhnliches Systemverhalten, schlechte Performance, große Dateien, Virenscanner wird deaktiviert, ...
- Prophylaxe:
  - Installation neuer Software durch Rechteeinschränkung verhindern
  - Antiviren-Software nutzen
  - Ausgehenden Datenverkehr überwachen (Egress filtering)

Quelle: Verizon Business

Bedrohung Nr. 15: Phishing und Variationen

- Angriffsmethodik:
  - Benutzer wird z.B. über eine E-Mail mit gefälschter Absendeadresse auf den Webserver eines Angreifers gelockt
  - Die Webseite sieht wie die eines bekannten, vertrauenswürdigen Dienstes aus (z.B. Internet-Banking, Online-Shopping, ...), dient aber nur dazu, Benutzername/Passwort und ggf. andere Daten des Benutzers abzugreifen
  - Relevant in 4% der Vorfälle und für 4% (!) der gestohlenen Daten
- Angriffserkennung:
  - Seltsame Aufforderungen, z.B. zur Datenkorrektur bei einer Bank, per E-Mail; häufig mit vielen Grammatikfehlern
- Prophylaxe:
  - Sensibilisierung der Benutzer
  - Links in E-Mails genau prüfen, HTML-E-Mails als reinen Text anzeigen
  - Firmenweit keine ähnlichen Aufforderungen selbst per E-Mail schicken

Quelle: Verizon Business