

- Heise Security, Meldung vom 2. Oktober 2005:
 - „Die Website von OpenSUSE ist derzeit offenbar gehackt. man bekommt hier eine Meldung der IHS Iran Hackers Sabotage zu sehen, die das Atom-Programm des Iran verteidigt.“



Quelle: www.zone-h.org

- Was für Mittel hätten Sie, um den Verlauf dieser Attacke in ihrem e-Business-Portal nachzuvollziehen?
- Welche Logdateien stehen in Ihrer e-Business-Anwendung für forensische Untersuchungen zur Verfügung?

Forensische Untersuchungen in e-Business-Portalen

Jan P. Monsch
jan.monsch@csnc.ch

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

- Ausgangslage
- Fall 1
 - Web-Site-Defacement
 - Zentrales Logging
- Fall 2
 - Phishing-Attacke
 - Korrelation von Logdateien
- Fall 3
 - Feststellungen aus Security-Reviews von Web-Applikationen
 - Logdateien und ihr Zielpublikum
 - Inhalte von Logdateien
 - Transaktionsverhalten beim Logging
- Monitoring

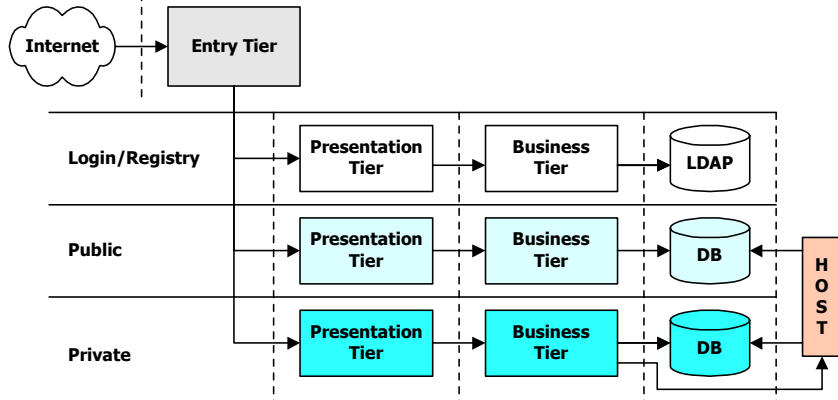
Ausgangslage

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

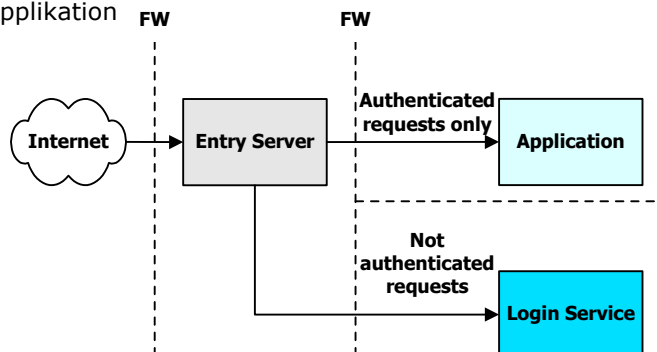
Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

- Fragen, die bei einer forensischen Untersuchung beantwortet werden müssen
 - **Ist ein Vorfall eingetreten?**
 - Feststellen des Vorfalls
 - Prüfen der Echtheit des Vorfalls
 - **Was** ging verloren?
 - Welche Informationen wurden gestohlen oder manipuliert?
 - Welche Kunden sind betroffen?
 - **Wie** war der Ablauf des Vorfalls?
 - **Wann** ist es geschehen?
 - **Wer** ist am Vorfall beteiligt?
 - Welche IP-Nummern sind am Vorfall beteiligt?
 - Ist ein bekannter Benutzer am Vorfall beteiligt?
 - Ist die Benutzerkennung authentisch?

- Heutige e-Business Portale sind hochgradig verteilte Anwendungen und Loginformationen entstehen auf mehreren Systemen in verschiedenen Tiers und Zonen



- Entry-Server
 - terminiert die SSL-Verbindungen
 - lässt die Anmeldung über zentralen Login-Service abwickeln
 - lässt nur authentifizierte Requests auf die Applikation zu
 - über gibt den Principle (Benutzer-Id) als Request-Header der Applikation



- Schwierigkeiten
 - Nicht jedes System in einem Portal hat alle Informationen, um die forensischen Fragestellungen zu beantworten
 - Die Log-Informationen, falls überhaupt vorhanden, sind über mehrere Systeme verteilt

 - In der öffentlichen Zone (Public Zone)
 - Nur die IP-Nummer des Client-Systems lässt sich zweifelsfrei bestimmen.
 - Merkmale wie UserAgent- und Proxy-Via-Header können weitere Details liefern, sind jedoch keine zuverlässigen Identifikationsmittel.

 - In der Kunde-Zone (Private Zone)
 - Es lassen sich sowohl IP-Nummer wie auch die Benutzer-Id bestimmen
 - Qualität der Identifikation des Benutzers hängt von der Qualität des Authentisierungsverfahrens ab.

- Die 3 Authentisierungsfaktoren
 - Wissen
 - Passwort, PIN, ...
 - Besitz
 - Smart-Card, SecurId, Safeword, Vasco, OTP, ...
 - Sein
 - Fingerabdruck, Iris, Sprache, Gesicht, ...

- Starke Authentisierung
 - Kombination von mindestens 2 Faktoren

- Qualität der Authentisierungsverfahren gegenüber Hacker-Angriffen

Authentication method	Hacker Capabilities		
	Keystroke sniffer	Keystroke sniffer Download file	Full Control by MMC Remote Admin
UN, PW	long	long	long
UN, PW, OTP	short	short	short
Cert on HD, PIN	-	long	long
Cert on HD, PIN, OTP	-	short	short
Cert on Smartcard, PIN entered on PC keyboard	-	-	long
Cert on Smartcard, PIN entered on reader keyboard	-	-	-

UN = Username
 PW = Password
 OTP = One-Time-Password (SecurId, Safeword, OTP)
 Cert = Client Certificate
 HD = Harddisk
 MMC = Malicious Mobile Code

- Eine Benutzer-Id in einer Logdatei sagt noch nichts darüber aus, ob es wirklich die Person war, die zur Benutzer-Id gehört!

Fall 1 - Web-Site-Defacement

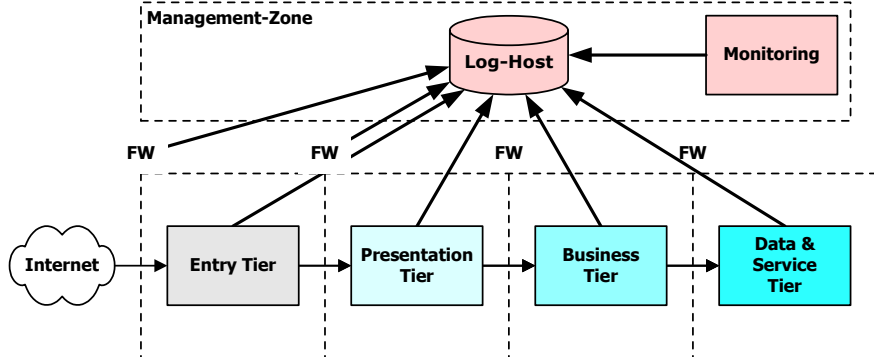
GLÄRNISCHSTRASSE 7
 POSTFACH 1671
 CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
 Fax+41 55-214 41 61
 team@csnc.ch www.csnc.ch

- Vorfall
 - Einer Hacker-Gruppe gelang es die Web-Site einer Bank für 30 Minuten zu verunstalten
 - Plazierung einer neuen Web-Server-Konfiguration und einer Web-Seite mit der Defacement-Meldung in einem temporären Verzeichnis
- Architektur
 - Reverse-Proxy vor Web-Server
 - Tripwire war auf allen System installiert, jedoch die temporären Verzeichnisse waren nicht geschützt
 - Web- und Applikations-Server waren nicht auf dem aktuellsten Patch-Level
- Erkennung der Attacke
 - Durch Kunden und interne Mitarbeiter

- Problematik
 - Reverse-Proxy
 - Festplatte wurde zur Analyse in ein Test-System mit RAID-Controller eingebaut
 - Durch das RAID-Recovery wurde die Festplatte überschrieben und somit wurden die Beweismittel gelöscht
 - Web-Server
 - Bis auf die aktuellen Log-Dateien waren alle Dateien vorhanden
 - Die Log-Dateien wurden durch die Angreifer absichtlich gelöscht
 - Nur die Loginformationen nach dem Vorfall waren vorhanden
 - Durch Dateiforensik konnten nur noch Bruchstücke der gelöschten Logdateien wieder hergestellt werden.
 - Kein Syslog war aktiviert
 - Kein IDS war installiert in der DMZ

- Damit Logeinträge nicht verloren gehen sollten diese zentral gespeichert werden
- Über ein Monitoring-System sollte die Log-Dateien überwacht werden



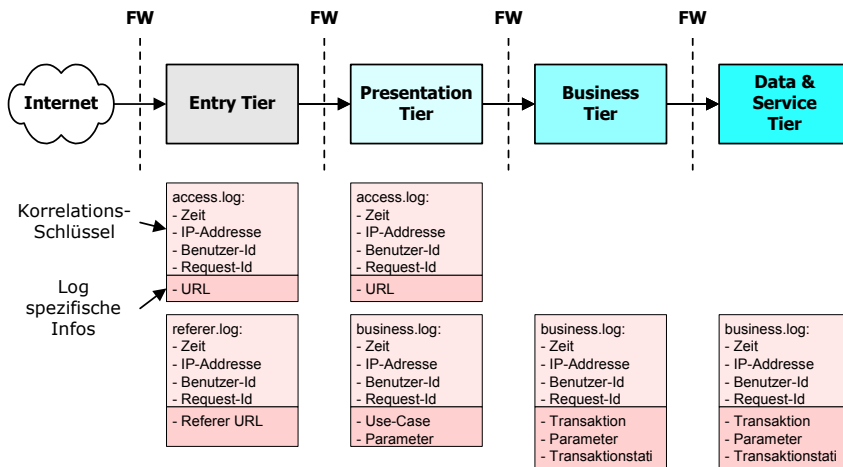
Fall 2 – Phishing-Attacke

- Vorfall
 - Offsite-Phishing-Attacke auf eine Online-Bank
 - Die Web-Seiten der Phishing-Web-Site enthielten verlinkte Bilder aus der Original-Web-Site
 - Angriff wurde Freitag Nachts gestartet
 - Über Redirect-Mechanismen von grossen Portalen wurden die Requests der Benutzer über hunderte russische virtuelle Web-Sites verteilt
- Erkennung der Attacke
 - Kunden haben die Attacke zuerst bemerkt und dies per E-Mail am Helpdesk gemeldet
 - Helpdesk war wegen des Wochenendes nicht dauernd besetzt
 - Es dauerte fast einen halben Tag bis reagiert wurde
 - Bis die ersten Gegenmassnahmen implementiert waren, dauerte es einen weiteren halben Tag

- Problematik
 - Gegenmassnahmen erfolgten nicht unmittelbar
 - Die Hacker-IPs konnten erst festgestellt werden, nachdem sich gehishte Kunden beim Helpdesk gemeldet haben
 - Über das Applikations-Log konnten die IP-Adressen der Hacker festgestellt werden.
 - Die IP-Adressen kamen aus der ganzen Welt
 - Referer-Logdatei war nicht vorhanden. Somit konnten die extern verlinkten Bilder und damit die Client-IPs, die über die Phishing-Site hereingekommen sind nicht erkannt werden
 - Kontakte zu Externen wie ISP oder CIRTs waren nicht vorhanden
 - Zufällig war ein Mitarbeiter anwesend, der russisch sprach und sich mit dem Virtual-Hoster in Russland verständigen konnte

- Damit die verschiedenen Logdateien zueinander korreliert werden können, müssen diese entsprechende Schlüssel enthalten
- Gängige Korrelationschlüssel
 - Zeit
 - Zentraler Synchronisationsservice nötig (NTP oder DCF-77)
 - Über die Zeit können Requests von verschiedenen Benutzern nicht auseinander gehalten werden
 - Delegation
 - der IP-Adresse des Clients durch alle Tiers hinweg
 - Requests können einem Client zugeordnet werden
 - von Benutzer-Id durch die Tiers hinweg
 - Requests einzelner Benutzer können verfolgt werden
 - von Request-Ids durch die Tiers hinweg
 - Einzelne Requests können gezielt verfolgt werden

- Korrelation über die Tiers hinweg (Darstellung vereinfacht)



- Die wichtigen Korrelationsschlüssel sollten über alle Tiers hinweg in (fast) allen Logdateien aufgezeichnet werden
 - Die Aufbereitung von Logdateien für eine computergestützte forensische Untersuchung ist viel weniger zeitintensiv
 - Für viele Fragestellungen muss nur ein Log ausgewertet werden und nicht mehrere
 - Verschiedene Logs haben verschiedene Lebensdauer; im Verlaufe der Zeit gehen sonst wichtige Informationen zur Korrelation verloren
 - Access-Logs werden häufig gerollt, z.B. 10 Logdateien à 10 MB
 - Business-Logs werden meist länger aufbewahrt, z.B. 200 Tage
- Die Übertragung der Korrelationsschlüssel zwischen den Tiers ist über Principle-Delegations-Mechanismen von Entry-Servern und J2EE-Container sehr einfach möglich

- Ausgangslage
 - e-Business-Anwendung schreibt zwar Logdateien, jedoch
 - Unverständliche Einträge in den Logdateien – ohne Hilfe des Entwicklers nicht nachvollziehbar
 - Unvollständige Angaben
 - Mehrzeilige Einträge oder Java-Stack-Traces
 - In schwer auszuwertenden Formaten wie XML
- Problematik
 - Fehlende Korrelationsschlüssel verunmöglichen eine End-to-End-Korrelation durch alle Tiers, was die "Chain of Evidence" unterbricht.
 - Die Einträge in den Logdateien sind nicht nachvollziehbar
 - Was hat der Benutzer genau gemacht?
 - Mehrzeilige Einträge für die gleiche Transaktion
 - Was gehört genau zu einer Transaktion?
 - XML-Dateien werden von gängigen forensischen Tools nicht automatisch verarbeitet und müssen manuell aufbereitet werden

- **Log einer Web-Applikation ohne sinnvolle Struktur**

```
LOG: [ch.csnc.lab.appsec.Login] Do login request: inputval3
LOG: [ch.csnc.lab.appsec.Login] Param username: hacker12
LOG: [ch.csnc.lab.appsec.Login] Param password: gugu.gugs
LOG: [ch.csnc.lab.appsec.login.Login] Param originalURL:
https://192.168.200.203/12001/inputval_case3/inputval3/control
ler?action=profile
LOG: [ch.csnc.lab.appsec.Login] Enter cookie scenario
LOG: [ch.csnc.lab.appsec.ServerUtilities] 1 cookies received
LOG: [ch.csnc.lab.appsec.Login] cookie name:  BCookie
LOG: [ch.csnc.lab.appsec.Login] session id:  null
LOG: [ch.csnc.lab.appsec.Login] session valid: false
LOG: 'java.naming.provider.url'='ldap://127.0.0.1:389/...'
LOG: 'java.naming.factory.initial'='com.sun.jndi.ldap.Lda...,
LOG: 'com.sun.jndi.ldap.connect.timeout' = '500'
LOG: 'java.naming.security.principal'='cn=hacker12,dc=b...
LOG: 'java.naming.security.authentication' = 'simple'
LOG: 'java.naming.security.credentials' = 'gugu.gugs'
EXCEPTION:      [LDAP: error code 49 - Invalid Credentials]
```

- Die Logdateien sollten dem Zielpublikum gerecht werden
- **Audit-Logs**
 - Zielpublikum: Customer Support, Revision & Security Office
 - Business Log: Geschäftsvorfälle
 - Security Log: Sicherheitsrelevante Logs
- **Access-Logs**
 - Zielpublikum: Betrieb, Security-Office
 - Aufzeichnung der Web-Site-Zugriffe
- **Referer-Logs**
 - Zielpublikum: Betrieb, Security-Office
 - Aufzeichnung der Referer-URLs

- Statistik-Logs
 - Zielpublikum: Marketing
 - Statistische Informationen
- Error-Logs
 - Zielpublikum: Betrieb
 - Applikatorische Fehler, die für den Betreib notwendig sind
- Debug- oder Trace-Logs
 - Zielpublikum Entwickler
 - Enthält ausführliche Debug-Informationen, die nur durch den Entwickler verstanden werden können

- Business Log
 - Aufzeichnung der Geschäftsvorfälle
 - Request, welcher das Geschäft angestossen hat.
 - Parameter, die in die Transaktion hineingegeben wurden.
 - Resultate der Transaktion, wie Statusinformation, ob erfolgreich oder nicht und allfällige Rückgabewerte
- Security Log
 - Enthält Informationen über erfolgreiche oder fehlgeschlagene Sicherheitsoperationen
 - Login und Logout des Benutzers
 - Passwortänderungsvorgang
 - Prüfung der Autorisation auf Funktion oder Daten
 - Änderungen in Benutzerprofilen

- Informationen, die nicht in eine Logdatei gehören
 - Passwörter (egal ob als Klartext, Verschlüsselt oder Hash)
 - Verschlüsselungsmaterial (z.B. SSL-Schlüsselmaterial)
 - Kritische Personendaten und -profile
 - Kundennamen

```
192.168.200.63 - - [26/Aug/2004:14:47:48 +0200] "GET /12001/inputval_case2/auth_inputval2/login?username=ha  
cker10&password=compass&action=login&originalURL=https  
%3A%2F192.168.200.203%2F12001%2Finputval_case2%2Finput  
val2%2Fcontroller%3Faction%3Dprofile&send=anmelden  
HTTP/1.1" 302 0
```

- Logdateien werden häufig zu Debugging-Zwecken an Lieferanten oder Entwickler weitergereicht.

- Das bedeutet, dass
 - URLs diese Informationen nicht enthalten dürfen , den sonst werden diese im Access-Log gespeichert
 - Solche Requests dürfen nur über die HTTP-Methode Post abgewickelt werden
 - Um trotzdem eine Nachvollziehbarkeit der Objektzugriffe in der Logdatei zu erhalten sollten die jeweiligen Datenbank-Primärschlüssel der Objekte geloggt werden
 - Sprechende Benutzernamen (jmonsch) sollten durch anonyme technische Ids (452312) ersetzt werden.

- Das Transaktionsverhalten bei Audit-Logs ist sehr wichtig
 - Es müssen Audit-Logs vor und nach ein Geschäftstransaktion geschrieben werden
 - Bei einem Crash der Applikation geht ansonsten die Information des Transaktionsstarts verloren
 - Treten beim Schreiben und Flushen der Logeinträge Fehler auf, so muss die Transaktion abgebrochen werden
 - Verhindert Situationen, wo Transaktionen durchgeführt werden ohne dass Logeinträge geschrieben werden.

- Beispiel einer Implementation (Darstellung vereinfacht)

```
public static final TRADE = "issueTrade";

public issueTrade(Session session, RequestObject req,
ResponseObject resp) throws Exception {
    try {
        Audit.log(TRADE, request.getUniqueId(),
            session.getUser(), Audit.START, req);
        brokerage.issueTrade(request, response);
        Audit.log(TRADE, request.getUniqueId(),
            session.getUser(), Audit.END_SUCCESS, resp);
    }
    catch (Exception ex) {
        Audit.log("issueTrade", session.getUser(), null,
            Audit.END_FAIL, ex);
        throw new AbortRequestException(ex);
    }
}
```

Monitoring

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

- Nebst forensischen Untersuchung erlauben Logininformationen auch das aktive Monitoring von verdächtigen Sachverhalten...
- Security-Log
 - Überwachung von Autorisationsverletzungen
 - Hacking-Versuche
 - Fehlkonfigurationen oder Bugs in Anwendungen, die auf Informationslecks hinweisen könnten
 - Übermassig hohe Anzahl von Login-Fehlern
 - pro Benutzer: Passwort-Brute-Force-Attacken
 - pro System: Benutzer-Enumeration oder Denail-of-Service-Attacken
- Business-Log
 - Unüblich grosse Anzahl von Transaktionen bei einem Benutzer können auf Denail-of-Service-Attacken hinweisen
 - Fehlgeschlagene Transaktionen weisen auf Verfügbarkeitsprobleme von Backend-Systemen hin.

- Access-Log
 - Aufruf von unbekanntem URLs kann ein Hinweis auf URL-Enumerations-Attacken sein

- Referer-Log
 - Feststellung von Verlinkung von Inhalten (z.B. Bildern) in fremden Web-Siten.
 - Hinweise auf eine Offsite-Phishing-Attacke sein.
 - Urheberrechtlicher Missbrauch von Inhalten in fremden Web-Seiten

- Um forensische Untersuchungen in e-Business-Portalen zu ermöglichen, sind vorgängig Massnahmen im Bereich des Logging zu treffen.

- Ein ausgereiftes Logging-Konzept und eine durchgängige Umsetzung sind daher Basis für erfolgreiches Monitoring UND erfolgreiche forensische Untersuchungen!



**GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL**

**Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch**