IT-Security: Organisation und Richtlinien in der Praxis

Gabriel Lottaz
IT-Fachverantwortung Netzwerk & Security
Migros Ostschweiz
gabriel.lottaz@gmos.ch

IT - Security Forum #5

Agenda

- Rückblick
- Organigramm & Verantwortlichkeiten
- IT-Security Newsletter
- Benutzer-Richtlinien
- Technische Massnahmen
- Links

Rückblick – Virus & Wurm

- 19. Januar 1986
  - 1. PC Virus: ©Brian (Bootsektor Virus)
    - Lahore, Pakistan
- 2. November 1988
  - 1. Internet Wurm
    - Legte das Internet lahm
    - Autor: Robert Morris Jr.
      - von der „Effizienz“ seines Werks überrumpelt

Rückblick - GMOS

- 1989
  - Aufbau der LAN Infrastruktur
- 1992
  - GMOS: TCP/IP Netz & Dienste (NextStep)
- Juni 1995
  - Internetanbindung
    - TIS Firewall Toolkit (Open Source)
    - 1 System als Firewall & Gateway

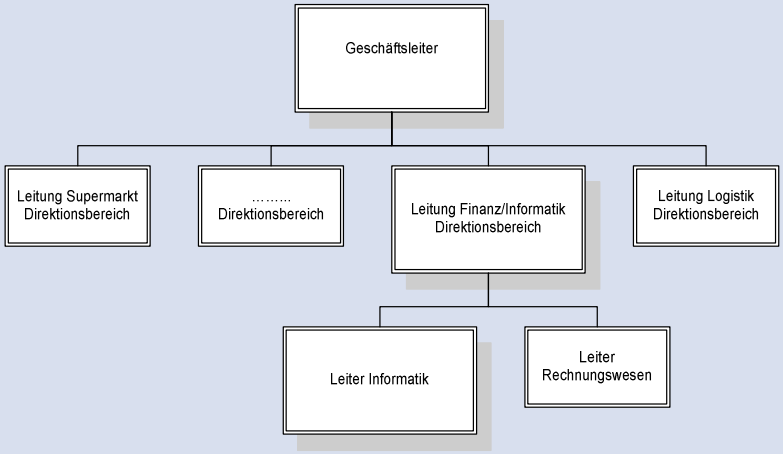
Rückblick

- 4. Mai 2000
  - Loveletter (VBScript)
    Virusname: Loveletter.a
    Subject: ILOVEYOU
    Message: kindly check the attached LOVELETTER coming from me.
    Attachment: LOVE-LETTER-FOR-YOU.TXT.vbs
  - keine Auswirkungen in der GMOS
    - Betriebssystem NextStep im Einsatz
- Mai 2001
  - Umstellung auf Windows 2000
  - Virenscanner und neue Proxy eingeführt
  - Aufwand in Security nimmt zu

Agenda

- Rückblick
- **Organigramm & Verantwortlichkeiten**
- IT-Security Newsletter
- Benutzer-Richtlinien
- Technische Massnahmen
- Links

Organigramm



Verantwortung

- liegt bei der Geschäftsleitung
  - diese kann delegieren an
- Direktor Finanz/Informatik
  - dieser kann delegieren an
- Leiter Informatik
  - dieser kann die Verantwortung
  - … nicht mehr weiterdelegieren

Änderungen von Security-Rules

- aus einem Projekt
  - bei kritischen Änderungen
    - Diskussion
    - Eskalation an IT-Leiter
- IT-Auftrag
  - Beurteilung durch IT-Security Fachgruppe
  - Bewilligung des IT-Leiter
- Schwerwiegende Entscheide
  - Information der Geschäftsleitung

IT - Security Forum #5

29

Verantwortung der Teams

- IT Teams
  - sind für Ihre Produkte / Systeme zuständig
  - Security bildet hier keine Ausnahme
- Fachverantwortliche IT Security
  - informieren sich über Security Alerts (Bugs)
  - beurteilen der Security Alerts
  - Software im Einsatz ?
    - Schadenspotential für GMOS
      - SW / System kommuniziert im Internet (z.B. Webbrowser)
  - Eskalation bei kritischen Bugs
  - erstellen IT-Security Newsletter

IT - Security Forum #5

30

IT - Security Forum #5

Agenda

- Rückblick
- Organigramm & Verantwortlichkeiten
- **IT-Security Newsletter**
- Benutzer-Richtlinien
- Technische Massnahmen
- Links

IT - Security Forum #5

IT-Security Newsletter

- monatlich
- Viren & SPAM Statistik

	Mailgateway (Email)	http/ftp Gateway	Virenscaner Exchange	Virenscaner Fileserver	Virenscaner (Clients)
Spam	16'893 (15.2 %)	-	-	-	-
gelöschte Anhänge	43	-	-	-	-
Viren	5'818 (5.3 %)	2	0	0	0
Blockierte Spyware	-	8'785 (41.2 MB)	-	-	-

- Bericht über Zwischenfälle und Störungen
  - falls ein Virus auf Client entdeckt wurde
  - Störung der Sicherheits-Infrastruktur

IT-Security Newsletter

- Liste der neuen Security Alerts
  - Einteilung in Risikostufen

Risikostufe		Massnahmen / Vorgehen
NOTFALL	sehr grosses Risiko	unverzügliche Reaktion notwendig
KRITISCH	grosses Risiko	Fall muss aktiv überprüft werden (wöchentlich); Termin für Patch ist zwingend einzuhalten
MITTEL	Risiko vorhanden	Fall muss monatlich überprüft werden
NIEDRIG	geringes Risiko	Fall wird nicht aktiv weiterverfolgt; Patch ist möglichst im normalen Releasemanagement einzuspielen

  - Beschreibung des Bug
  - Lösungsbeschreibung (meistens Patch)
  - Empfehlung
  - Termin

Eskalation bei kritischen Bugs

- Zuständiges Team wird sofort beigezogen
- Lage zusammen analysiert
- Abwiegen der Risiken
  - Gefahr für ganzes Unternehmen ?
  - Wichtigkeit des betroffenen Systems
  - übereiltes Patchen auch riskant !
  - Entschärfung durch andere Massnahmen
- Einstufung zusammen festgelegt
- Bei Uneinigkeit wird eskaliert
  - Entscheid durch IT-Leiter

Agenda

- Rückblick
- Organigramm & Verantwortlichkeiten
- IT-Security Newsletter
- **Benutzer-Richtlinien**
- Technische Massnahmen
- Links

IT - Security Forum #5

35

Benutzer-Richtlinien

- regeln Nutzung der Informatik Infrastruktur
- regeln private Nutzung des Internets
- geben Hinweise zur Vertraulichkeit
- regeln Übernahme der Benutzersession
- definieren Anforderungen an das Passwort
- geben Verhaltensmassregeln zum Virenschutz

- sind Bestandteil der Hausordnung !
- aktuelle Version ist im Intranet

IT - Security Forum #5

36

Private Nutzung des Internet

- Ausserhalb der Arbeitszeit erlaubt
- Produktion darf nicht beeinträchtigt werden
- Verboten
  - Downloads von Dateien
  - Musik- und Filmwiedergabe (Streaming)
  - Chatten
  - Versenden von grossen Email-Anhängen
  - Auktionen (eBay)

IT - Security Forum #5

37

Hinweis zur Vertraulichkeit

- Protokollierung des Datenstroms
  - Email- und Webverkehr wird protokolliert
  - Erstellung von Statistiken
  - Zugriff auf Logdaten streng eingeschränkt
- Überwachung der Benutzer
  - Nur nach ausdrücklicher Information erlaubt
  - Datenschutzgesetz
  - Verordnung 3 des Arbeitsgesetzes Art. 26

IT - Security Forum #5

38

Übernahme der Benutzersession

- wichtige Funktion zur Hilfestellung
  - Erleichtert Unterstützung der Benutzer
  - Arbeitssitzung des Benutzers betrachten
  - Arbeitssitzung aktiv übernehmen
- Heikel in Bezug auf Daten- & Persönlichkeitsschutz
- Massnahmen
  - Benutzer autorisiert Übernahme
  - Übernommene Arbeitssitzung für Benutzer ersichtlich

Virenschutz

- Benutzer sensibilisieren !
  Begriff und Schadenspotential erklären
- Verhaltensregeln
  - Alle externen Datenquellen scannen (geschieht beim Lesen der Daten automatisch)
  - Email-Anhang von Unbekannt ungeöffnet löschen
  - Bei Verdacht auf Virus unverzüglich Helpdesk informieren
  - Virus-Warnung nicht weiterverbreiten
    - Hoax (Kettenmail)

Agenda

- Rückblick
- Organigramm & Verantwortlichkeiten
- IT-Security Newsletter
- Benutzer-Richtlinien
- **Technische Massnahmen**
- Links

IT - Security Forum #5

41

technische Massnahmen

- Firewall
  - mehrere Interfaces / VLAN
  - zwei Stufen - ein Produkt
- Email-Gateway
  - Virenscanner
  - SPAM Filter
  - entfernt ausführbare Anhänge

IT - Security Forum #5

42

technische Massnahmen

- Web-Proxy mit Content Security
  - URL Filter: Sperren gewisser Kategorien
  - Virenscanner
  - SSL Proxy
    - entschlüsselt SSL-Verkehr
    - erlaubt die Überprüfung des Inhalts
    - überprüft Server Zertifikat
- Citrix Umgebung
  - restriktive Konfiguration
- Tool kontrolliert Ausführung von Programmen
  - muss von Administrator installiert worden sein

Agenda

- Rückblick
- Organigramm & Verantwortlichkeiten
- IT-Security Newsletter
- Benutzer-Richtlinien
- Technische Massnahmen
- **Links**

Links – Security Alerts

- SANS
  - http://isc.incidents.org
  - Newsletter
    @RISK: The Consensus Security Vulnerability Alert
    https://portal.sans.org/preferences.php
- Heise Security
  - http://www.heise.de/security/news/alerts.shtml
- CERT
  - http://www.cert.org
- FrSIRT
  - http://www.frsirt.com

Links – Informationen

- SANS Security Policy Project
  - http://www.sans.org/resources/policies/
- BSI
  - Leitfaden IT-Sicherheit
    http://www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf
  - Dokumente zur IT-Sicherheit
    http://www.bsi.de/fachthem/sinet/dokumente.htm
  - IT-Sicherheit verständlich erklärt
    http://www.bsi-fuer-buerger.de
  - Musterrichtlinien u.a.
    http://www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf