swisscom fixnet
Einfach verbunden.

Informationstechnologie: Risikoanalysen in einem schnell sich verändernden Umfeld

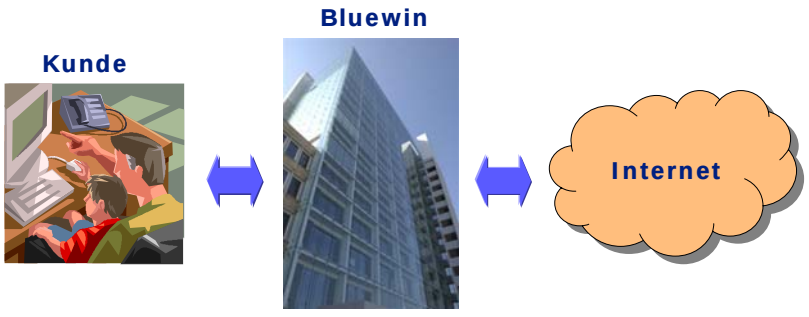
Charles d'Heureuse / Susanne Weidmann FX-BW-IT

27. April 2005

bluewin

swisscom fixnet
Einfach verbunden.

Wer ist Bluewin?



bluewin

Wer ist Bluewin?

swisscom fixnet
Einfach verbunden.

Mission

Geschäftsfelder:	**Internet Access, Portal, Internet Services, Broadband Services (Triple Play)**
Geschäftsgrundsätze:	**Standardprodukte, Leadership im Markt**
Kunden:	**Internetnutzer und –anbieter, Privat- und Geschäftskunden**
Leistungsversprechen:	**„Friendly Guide" im Internet**

Bluewin Ende 2004

- ⇨**1 Million aktive Access-Kunden**
- ⇨**435'000 ADSL-Kunden**
- ⇨**150 Millionen Pageviews pro Mt.**
- ⇨**100 % Geschäftsbereich der Swisscom Fixnet**

Führender ISP der Schweiz

bluewin

Inhaltsverzeichnis

swisscom fixnet
Einfach verbunden.

bluewin

swisscom fixnet
Einfach verbunden.

Welchen Gefahren sind wir ausgesetzt?

Wasseralarm Sihlsee

Die Talsperren des Sihlsees werden durch Vorrichtungen vor Beschädigungen geschützt. Sollten diese wider Erwarten trotzdem einen grösseren Schaden erleiden, so könnten die Wassermassen durch das Sihltal und in Gebieten links und rechts der Limmat in die Stadt Zürich fliessen.

Bei vollständiger und sofortiger Zerstörung der Talsperren könnten die auf dem Stadtplan bezeichneten Stadtteile bis zu 8 Meter unter Wasser gesetzt werden. In der meistgefährdeten Zone würden Gebäude durch Unterspülung der Fundamente oder durch den Anprall schwimmender Trümmer einstürzen. Die Flutwelle würde die Stadtgrenze in Leimbach in 1 Stunde und 25 Minuten, das Stadtzentrum in 1 Stunde und 50 Minuten nach dem Bruch der Talsperren erreichen. Die Ueberflutung würde voraussichtlich 4 bis 5 Stunden dauern.

Alarmsignal:

Bei allfälliger Zerstörung der Talsperren des Sihlsees wird die Bevölkerung in den überflutungsgefährdeten Gebieten der Stadt Zürich durch die Auslösung des Allgemeinen Alarms alarmiert. Der Allgemeine Alarm besteht aus einem an- und abschwellenden Heulton von 1 Minute. In diesem Fall ist sofort **Radio DRS1** einzuschalten, welches die Verhaltensmassnahmen bekanntgibt.

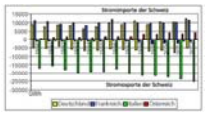
Stromausfall Italien

Italien:

Der grösste Stromausfall in der Geschichte Italiens hat am **28.09.2003** das ganze Land von Südtirol bis nach Sizilien lahmgelegt. 57 Millionen Italiener tappten im Dunkeln.

Schweiz:

Ist ein solch grosser Stromausfall auch in der Schwei möglich?



Terroranschläge

Quelle: Polizeidepartement des Kanton Zürichs für Schutz und Rettung

Die Kantonalen Polizeiorgane haben jederzeit die Möglichkeit, das diensthabende DRS Radiostudio zu verpflichten, unverzüglich eine Sonderdurchsage mit Verhaltensanweisungen und Informationen an die Bevölkerung des betroffenen Gebietes zu verbreiten. Die Bevölkerung in diesem Gebiet wird mittels Sirenen aufgefordert (Allgemeiner Alarm), Radio zu hören.

Erdbeben

Erdbebenrisiko in der Schweiz:

- **Erdbeben können in der Schweiz Katastrophen auslösen, wie sie keine andere Naturgefahr in vergleichbarem Ausmass bewirken könnte.** (Studie des Bundesamts für Zivilschutz)
- **In der Schweiz kann davon ausgegangen werden, dass sich schwere Erdbeben im Mittel alle 1'000 Jahre ereignen. Es bestehen jedoch regionale Unterschiede in der sogenannten seismischen Gefährdung.**

swisscom fixnet
Einfach verbunden.

Welchen Gefahren sind wird ausgesetzt?
Durch Individuen

- **Offenlegung von Informationen**
  - Ungewollt durch Fehlbedienung / Unachtsamkeit
  - Durch nicht Aktualisierung von Systemen
  - Durch ungenügende Absicherung der Kommunikation / Authentisierung
- **Beeinträchtigung des Dienstes**
  - Der Dienst wird „zerstört“
  - Der Dienst wird so beeinträchtigt das er nicht mehr benutzt werden kann
- **Daten werden manipuliert**
  - Daten werden nicht zerstört aber verändert
  - Finanzieller Verlust durch Manipulation der Date

⇨ Dies kann zu finanziellem Verlust und / oder Imageverlust führen

Wer kann / will uns Schaden zufügen?

- **Professioneller Hacker**
  - Eher unwahrscheinlich da Bluewin (noch) nicht so interessantes Ziel
  - Mit den zukünftigen Services (Voip, TV, VoD etc.) wird sich das ändern
- **„Normaler“ Hacker** (hat schon ein wenig Erfahrung)
  - Realistisch da er sich noch profilieren will
  - Jemand den Bluewin kennt und wir „verärgert haben“
- **Script Kiddies**
  - Versucht wird ständig
  - Grosse Gefahr, da Tools frei verfügbar und einfach zu bedienen sind (bekannte Schwachstellen ausnützen)
- **Normaler Benützer**
  - Der per Zufall etwas feststellt / einsieht und dies veröffentlicht
- **Fraudster / Spammer**
  - Spammer sind schon aktiv ⇨ Fraudster werden in Zukunft auftreten

Welchen Gefahren sind wird ausgesetzt?
Andere Bedrohungen

- **Imageschaden**
  - Das Thema Sicherheit ist komplex. Wirksame, verständlilche Oeffentlichkeitsarbeit ist daher enorm wichtig. Ein negativer Pressebericht (ob berechtigt oder nicht) kann viel Schaden anrichten.
- **„Empfundenes“ Risiko**
  - Nicht jede Bedrohung ist real. Aber sie kann vom Kunden als real empfunden werden und muss daher sehr ernst genommen werden.
- **Veränderliche Rechtslage**
  - Neueste Bundesgerichtsentscheide bezüglich Internet-Pronografie
  - Unsicherheiten bei SPAM & Co

Was können wir tun?

swisscom fixnet
Einfach verbunden.

Prävention

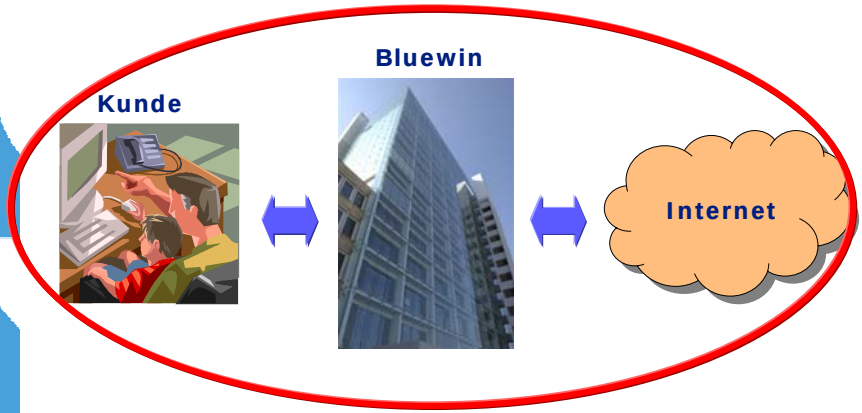
Intervention

Information

blu=win

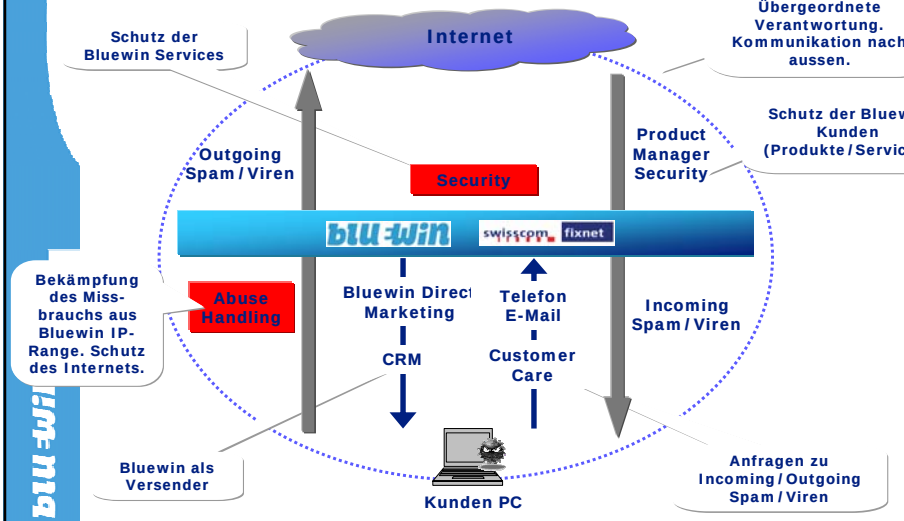
Wo können wir etwas tun?

swisscom fixnet
Einfach verbunden.



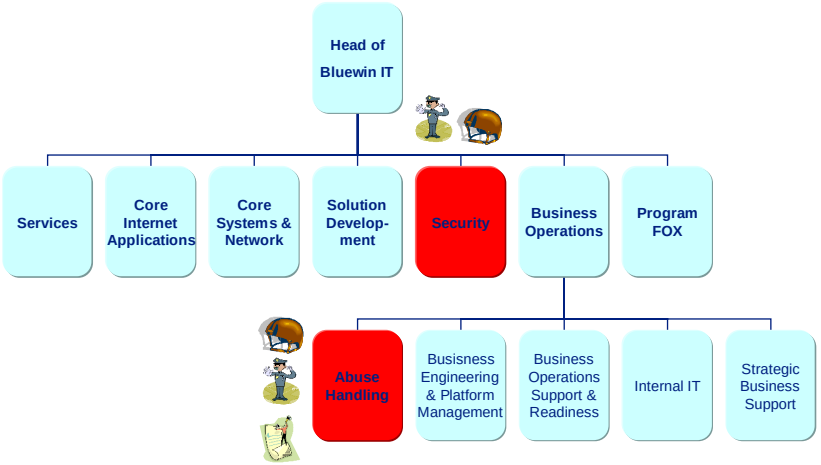
blu=win

Sicherheit
WAS wird heute WO durch WEN gemacht ?



Inhaltsverzeichnis

Wie ist die Bluewin für die Bekämpfung von Gefahren organisiert?



Inhaltsverzeichnis

Auftrag Security

swisscom fixnet
Einfach verbunden.

AUFTRAG

- Sicherstellen von **Netzwerk-, Daten- und Host-Sicherheit** sowie Überwachung der Sicherheit der Informationssysteme im Allgemeinen.
- Erstellen von **Richtlinien** und **operativen Vorgaben** zur **Daten- und Informationssicherheit** sowie der Überwachung von deren Ausführung.

Auftrag Abuse Handling

swisscom fixnet
Einfach verbunden.

AUFTRAG

- Abuse Handling **schützt das Internet und dessen Benutzer** vor **Missbrauch** ausgehend von Bluewin-Kunden, d.h. Kunden, deren IP-Adressen aus dem Bluewin-Netzbereich stammen.
- Mit **proaktiven Massnahmen** werden Bluewin-Kunden vor Missbrauch im Internet geschützt.

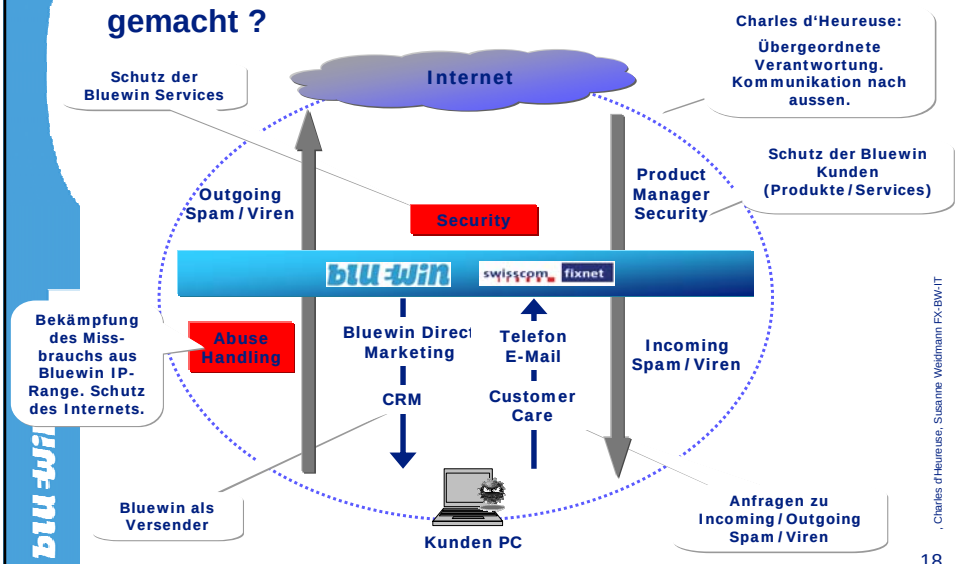
swisscom fixnet
Einfach verbunden.

Inhaltsverzeichnis

blu=win

swisscom fixnet
Einfach verbunden.

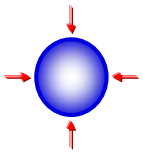
Sicherheit
WAS wird heute WO durch WEN gemacht ?



blu=win

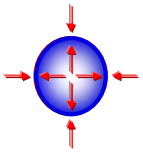
Schnittstellen und Abgrenzungen zwischen Security und Abuse Handling

- **Security** ist für den Schutz der produktiven Bluewin Infrastruktur und damit der Bluewin Services zuständig.



- **Abuse Handling** bekämpft Missbrauch aus dem Bluewin IP-Range zum Schutz des Internets.

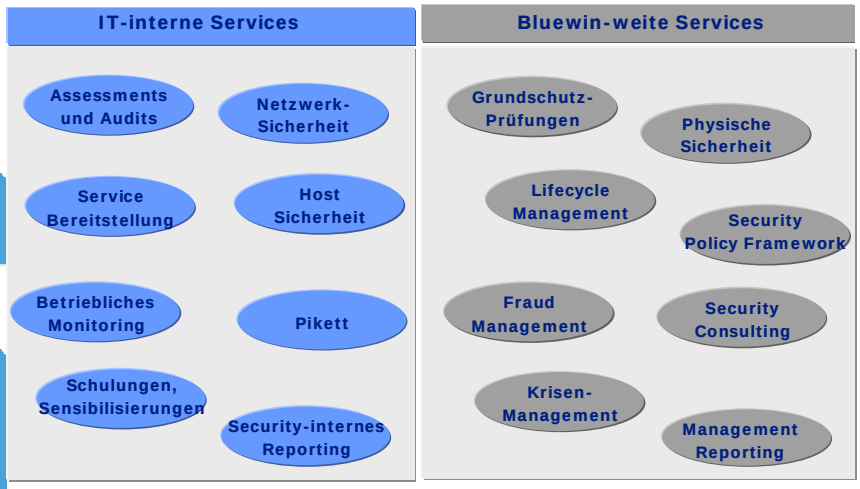
- Eine **Zusammenarbeit** zwischen **Security** und **Abuse Handling** erfolgt in denjenigen Bereichen, in denen Bluewin Produktionssysteme betroffen sind, beispielsweise im Fraud Management.



Inhaltsverzeichnis

Übersicht der Security-Tätigkeitsgebiete

swisscom fixnet
Einfach verbunden.



bluewin

Bluewin-weite Security Services 1/2

swisscom fixnet
Einfach verbunden.

- Jährliche Überprüfung aller Services auf Einhaltung der **Grundschutz-anforderungen**
- **Physische Sicherheit** (inkl. Katastrophenschutz)
- **Lifecycle Management** (LCM) über Projekte
  - Sicherheitsüberprüfung von Projekten und Services anhand von Checklisten
    - Security Anforderungen
    - Konzeptionelle Service-Überprüfung
  - Aufbau und Anpassung der Security Infrastruktur
- Unterhalt des **Security Policy Framework** (ISO 17779)

bluewin

Bluewin-weite Security Services 2/2

- **Security Consulting**
  - Allgemein
  - Infrastruktur (Bluewin Services)
  - Datenschutz, Informationssicherheit
  - Konzeptionelle Beratung
  - Hoher Zeitaufwand!
- **Fraud Management**
  - Sensibilisierung
  - Aufzeigen von Fraud Potential
- **Krisenmanagement**
- **Top Management und GL Reporting**
  - Periodische Reports
  - Statusberichte
  - Auditberichte

IT-interne Security Services 1/4

- **Assessments und Audits**
  - Vulnerability Assessments
    Scanning, Reporting, Trouble Ticket Management
  - Externer Audit (Komplettaudit)
    Für ganze produktive Infrastruktur (Bluewin Services)
  - Interne Audits durch das Security Team
    Dediziert für Services durchgeführt

IT-interne Security Services 2/4

- **Netzwerk-Sicherkeit**
  - Perimeter Schutz
    - Betrieb von Routers und Access Listen
    - Betrieb und Installation der Firewall Infrastruktur
  - Intrusion Detection
    - Angriffsüberwachung und –Monitoring
  - Netzwerk-Monitoring
    - Aufzeichnung des Netzwerk-Verkehrs mit dem Ziel der Sichtbarmachung von Forensics, Automatisierung im Aufbau
- **Host-Sicherheit**
  - Standarddefinitionen für Security und Gesamt-IT mit
    - Log-Auswertungen (zentrales Sys-Log)
    - Datenintegritätscheck
    - Hardening von Betriebssystemen (ausschliessliches zur Verfügung stellen von benötigten Funktionalitäten)

IT-interne Security Services 3/4

- **Service Bereitstellung**
  - Remote Access für Pikett leistende IT-Mitarbeiter, externe Partner-Mitarbeiter
  - Grundsatz „Single Point of Entry / Authentification“
  - Proxy Server Bereitstellung für Produktionsumgebung
    - mit Viren-Detektion für Uploads und Downloads für Produktionssysteme (Maintenance)
  - Jump Start Service
    - Automatisierte Installation (Basis Konfiguration) von Betriebssystemen: optimiert, gehärtet, 20 Minuten Installationszeit
- **Pikett** 7x24 für alle Security Themen
- **Betriebliches Monitoring** und **Incident Behandlung**

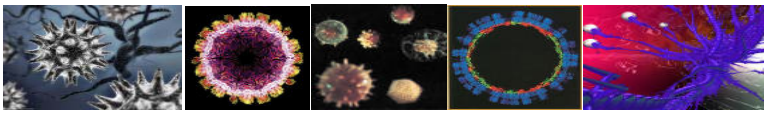
IT-interne Security Services 4/4

- **Betriebliche Auswertungen** für das Security Team (Daily Business)
  - Firewall Drop Monitoring
  - IDS (Intrusion Detection System) Alerts
  - Log-ins
  - Login-Failures
  - Proxy / RAS Verbindungsauswertungen
  - Syslog Auswertungen
  - Aktuelle Schwachstellen
- **Schulungen, Sensibilisierungen**
  - Grundsätzlich für alle Bluewin-Mitarbeiter
  - Fraud Schulungen für Product Managers

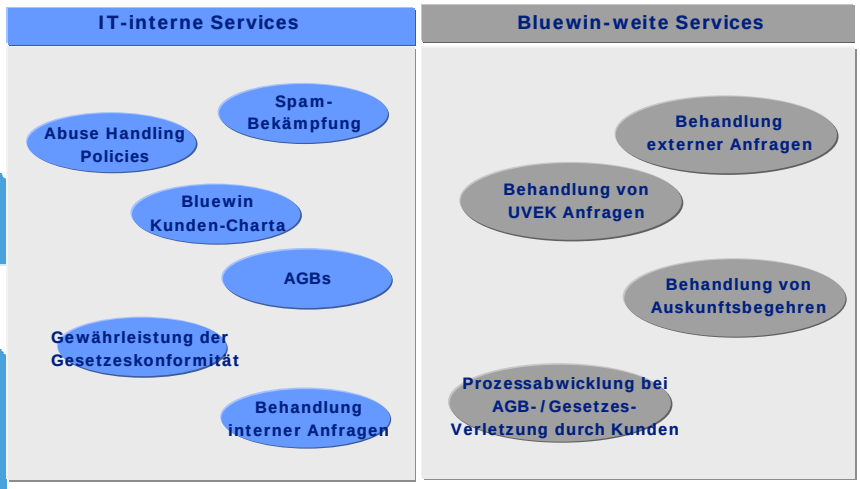
Grundsätzliche technische Security Anforderungen

- **Netzwerksicherheit**
  - Guter Perimeterschutz (erste Sicherheitsstufe)
  - Nur Traffic in / out, welcher wirklich für Services benötigt wird
  - Hohe Aktualität des Rulesets / der Accesslisten
  - Einhaltung der konzeptionellen Anforderungen
- **Hostsicherheit**
  - Sichere / aktualisierte Betriebssysteme
  - Es laufen nur benötigte Dienste
  - Tägliche Auswertung der Logs
  - Sicherherstellen das keine Files / Daten manipuliert wurden (Data Integrität)
  - ⇨ Dies gilt für alle Systeme
- **Applikationen**
  - Applikationen sollten aktuell sein
    - Keine bekannten High / Medium Risks
  - Bei Eingaben / Übergaben: Input Parameter Validierung
  - Authentisierung der Requests durch die Applikation

Inhaltsverzeichnis



Übersicht der Abuse Handling-Tätigkeitsgebiete



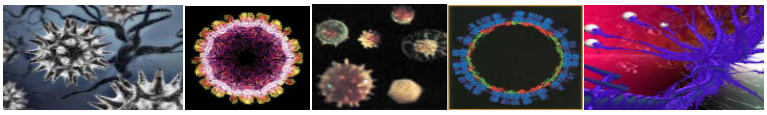
Bluewin-interne Abuse Handling-Services

- **Abuse Handling Policies**
  - Erstellen und Pflege von Abuse Handling Policies
- **Spam-Bekämpfung**
  - Single Point of Contact (SPoC) bei Projekten und Workshops
- **Bluewin Kunden-Charta**
  - SPoC
- **AGB**
  - SPoC für Bluewin interne Stellen im Zusammenhang mit AGB und Internet Missbrauch
- **Gesetzeskonformität**
  - Gewährleistung des gesetzeskonformen Agierens durch Bluewin bei Internet-Missbrauch
- **Anfragen intern**
  - Koordination von Anfragen innerhalb Bluewin zu Missbrauch im Internet

Bluewin-externe Abuse Handling-Services

- **Gesetzes- und Vertragskonformität**
  - Abwicklung von Prozessen bei Verletzung und Missachtung der Gesetz- und Vertragskonformität durch Kunden
- **Anfragen extern**
  - Bearbeiten von Eskalationen, Anfragen, kritischen Fällen sowie Grenzfällen betreffend Internet Missbrauch für die Bereiche Messaging, Hostcenter, MyPage und Broadband
- **Anfragen des UVEK**
  - SPoC für den Dienst für besondere Aufgaben des UVEK sowie die Koordinationsstelle Internet-Kriminalität im Bundesamt für Polizei KOBIK
- **Auskunftsbegehren**
  - Bearbeiten von Auskunftsbegehren gemäss Fernmeldegesetz

Spam und Viren – Aktuelle Entwicklung und Tendenzen



Spam und Viren – Generelle Entwicklung und Bluewin Inbound Traffic

Generelle Entwicklung*)

- Die globale Entwicklung zeigt:
  - 20% aller Enduser haben mindestens einen Virus auf ihrem Computer
  - 80% aller Enduser haben irgend eine Form von Spyware (Untergruppe von Trojaner) auf ihrem Computer
  - Laut einem Report von Panda Software im Februar 05 sind rund 35% aller PCs mit Viren / Würmern infiziert
- Erhöhtes Aufkommen von „Porno-Viren“ im Chatraum

Bluewin Inbound Traffic

- Zusammensetzung aus 50% Spam, 10% Worm, 0.1% Virus **)
- Die Netsky-Familie ist nach wie vor derjenige Wurm mit höchster Verbreitung

*) „Spam Zombies and Inbound Flows to Compromised Customer Systems“ von Joe St Sauver, MAAWG Senior Technical Advisor

**) Schätzungen von SC-INO / FX-BW-IT-MSG

Spam und Viren – Bluewin Outbound Traffic und Blacklisting

swisscom fixnet
Einfach verbunden.

Bluewin Outbound Traffic

- „Nigerianer Spam“, jedoch mit relativ geringem Volumen
- Eine neue Spam-Generation bricht an:
  - Noch sind Zombies aktiv (Trojaner mit eigener SMTP-Engine auf dem PC des Endusers spammt über Port 25 direkt ins Netz)
  - Der Spamversand erfolgt jedoch vermehrt wieder über ISP-Mailserver

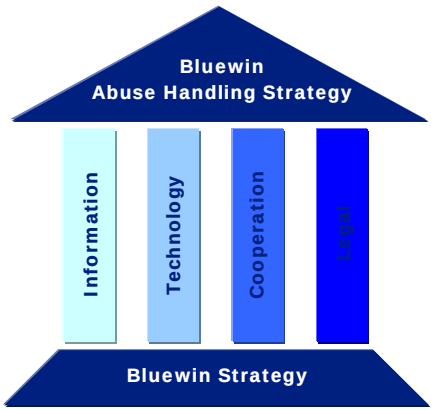
Blacklisting

- Vermehrte Listung dynamischer IP-Bereiche und Mailserver von Bluewin bei internationalen Blacklist-Anbietern
- Gravierendes Blacklisting Ende Februar 05 entstanden durch „Nigerianer Spam“
- „Nigeria-Taksforce“ für kurzfristige und erfolgreiche Entschärfung der Situation durchgeführt
- Weitere Massnahmen und Projekte für nachhaltige Spam-Bekämpfung sind definiert

bluewin

Massnahmen-Mix zur Spam-Bekämpfung

swisscom fixnet
Einfach verbunden.



bluewin

Aktueller Massnahmen-Mix

swisscom fixnet
Einfach verbunden.

Information

- Sicherheitsportal 1.0
- Medienberichte
- Flyers
- Interne Kommunikation (Intranet, Flyers, Post-it)
- **Sicherheitsportal als standardisierte Service Seite** neu

Kooperation

- ESP Work Group Anti-Spam (inoffiziell, formell)
- Indirekte Zusammenarbeit zwischen Bluewin und einzelnen Providern (keine Regelung)
- Swisscom ist Mitglied der Deutschen eco
- „Interconnection“ auf SysAdmin Ebene (Lead Bluewin)

Technologie

- Spam- und Virenfilter (Classic/Gold)
- Bluewin Firewall (Classic)
- Blacklisting mit Spamhaus.org
- Individuelles Blacklisting
- SMTP Authentisierung im Traveller Package
- **Projektanträge SMTP Auth / Port 25 Sperrung** neu
- **Sandbox in Umsetzung** neu
- **Erweiterte Quelle zur Angabe von infizierten Enduser-PC's im BW-Netz ⇨ können automatisch eskaliert werden** neu

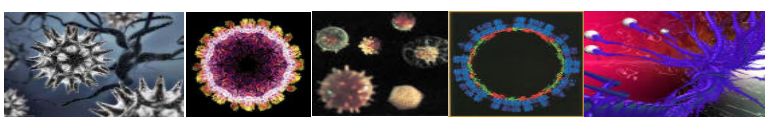
Recht

- **Neue Swisscom Fixnet AGB** neu
- Delegation für Diskussion mit Bakom

bluewin

Abuse Handling Mitarbeit in Fachgruppen

swisscom fixnet
Einfach verbunden.



bluewin

MAAWAG und ESP Anti-Spam Workgroup

MAAWAG

- Der **Beitritt** in die MAAWG ist initiiert.
- Das Abuse Handling Team von Bluewin war durch mit einem **Referat** am MAAWG General Meeting im März 2005 in San Diego vertreten. Behandelte Themen: Die Spam / Abuse Situation und die Entwicklung in Europa (Tendenzen, Massnahmen, Kooperationen etc.).

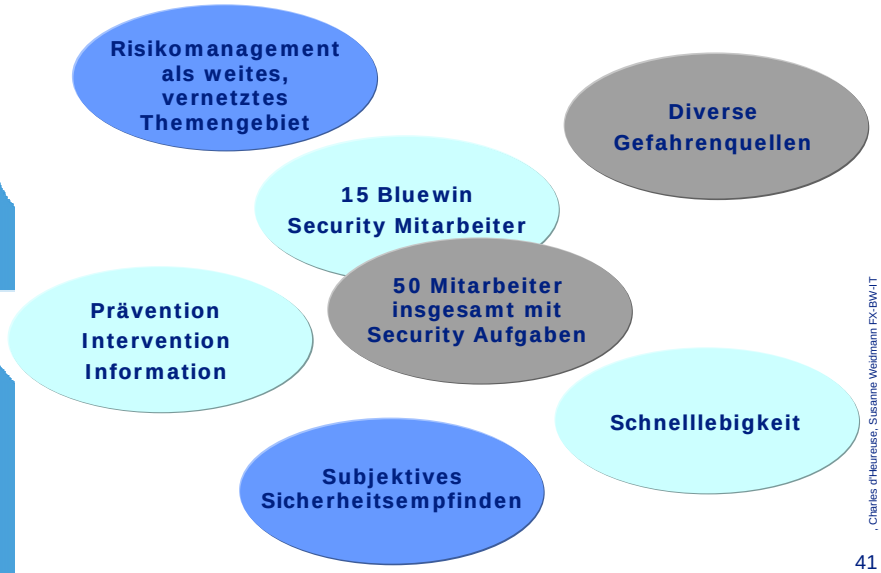
ESP

- **Ab April 05**
  - Kommunikation am Markt über gemeinsames Vorgehen
  - Implementierung gemeinsamer Massnahmen
    - Port25 Sperrung
    - SMTP Authentisierungen
    - Weitere gemeinsame Schritte und Massnahmen

Inhaltsverzeichnis

Zusammenfassung wichtiger Punkte

swisscom fixnet
Einfach verbunden.



bluewin

Fragen?

swisscom fixnet
Einfach verbunden.

bluewin