Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 83 (2005)

Heft: 3

Artikel: Ein umfassendes Sicherheitsmanagement

Autor: Bernhart, Christian

DOI: https://doi.org/10.5169/seals-877112

Ein umfassendes Sicherheitsmanagement

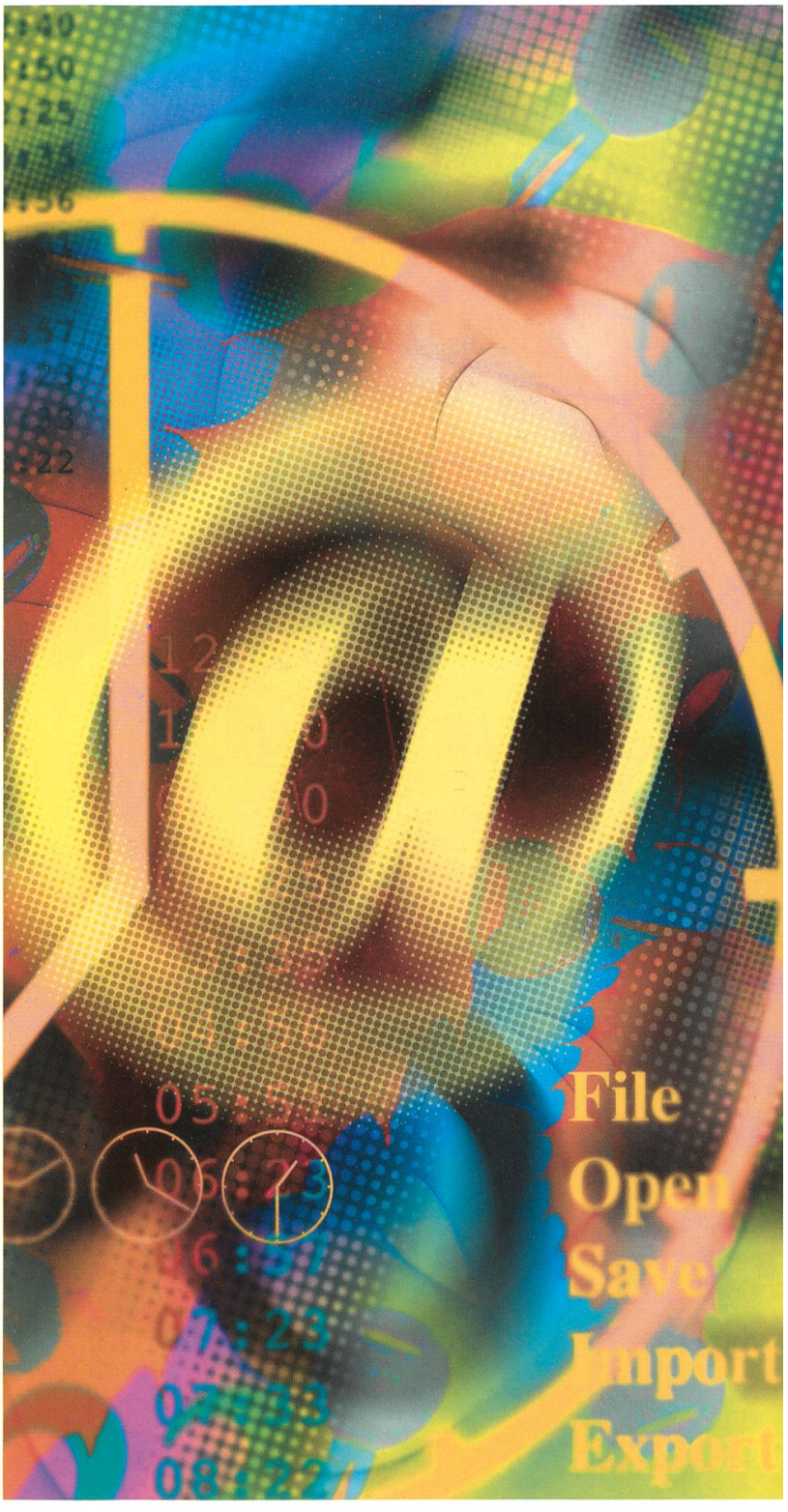
In allen Dienstleistungen, vom Telefon über Internet bis hin zu den IT-Services unterhält Swisscom ein umfassendes Sicherheitsmanagement, das von Swisscom Fixnet betreut wird. Neben der Installation entsprechender Software gehört dazu ebenso die Ausbildung, die Prozessanalyse sowie die in Audits verstärkte Sicherheitskultur der Mitarbeitenden.

Christian Neuhaus, Group Media Relations von Swisscom AG, stellte sich den Fragen, die der Journalist Christian Bernhart ihm zum Thema Sicherheit und Verfügbarkeit gestellt hat.

Herr Neuhaus, im technischen Bereich des ICT-Sicherheitsmanagements gibt es eine Palette von Firewall-Produkten und Virenscannern. Zeigt die Erfahrung, dass der parallele Einsatz von Produkten verschiedener Hersteller eine bessere Sicherheit gewährleistet?
Ja, Bluewin setzt seit Jahren mit Erfolg auf eine Multi-Vendor-Strategie im Bereich Sicherheit. Dies gilt für technische Produkte (Scanner, Firewalls usw.) wie für die Sicherheitsberatung und -architektur.

Gibt es dabei Kompatibilitätsprobleme, insbesondere im Internetverkehr?
Eigentliche Kompatibilitätsprobleme gibt es kaum. Aber wir sind im Residential-Markt tätig, das heisst, es muss uns gelingen, komplexe Zusammenhänge zwischen einzelnen Produkten zu erkennen und für den Kunden einfach und nachvollziehbar darzulegen. Soviel wir wissen, ist beispielsweise die Bluewin Firewall weltweit die erste Lösung, die ein ganzes Heimnetzwerk schützt, ohne dass der Kunde irgend etwas installieren muss. Wenn nun ein Betriebssystem auf einem PC diese Firewall noch nicht erkennt und eine entsprechende Warnung ausgibt, kann dies den Kunden verwirren. In diesem Fall können wir über unsere Customer-Care-Agenten Unterstützung bieten.

Welchen Einfluss hat das gewählte Betriebssystem auf die Sicherheit? Für die E-Vergabeplattform wählt Swisscom IT Services Linux. Sollte man auf mehrere Betriebssystem setzen?
Das Betriebssystem für E-Plattformen spielt heutzutage eine untergeordnete Rolle. Bei unseren Kunden setzen wir für viele Internetauftritte sowohl Linux bzw. Unix und vor allem Windows sehr erfolgreich ein. Entscheidungen der Architektur werden hauptsächlich durch die Applikation und die Businesslogik bestimmt. Die Voraussetzung in Bezug auf die Sicherheit und somit die Wahl des Betriebs-



systems unterscheiden sich nur marginal. Ein «gehärtetes» Betriebssystem mit einem gelebten Patchmanagement-Prozess sowie eine kompetitive Netzwerkzonenanbindung mit Reverse Proxy und Firewalls gehören heutzutage zum Standard.

Der ISDN-Anschluss reagiert auf Stromausfall mit einem Leitungsunterbruch. Ist das unter dem Aspekt der Verfügbarkeit ein Thema für Swisscom oder soll man dann einfach auf das Mobilnetz Zugriff nehmen?
Falls es zu einem Stromausfall kommt, schaltet das «ISDN NT2ab» in den so genannten Notbetrieb, was wiederum bedeutet, dass die Speisung nun vom Amt her erfolgt. Das «NT2ab» kann so konfiguriert werden, dass entweder der S-Bus oder die analoge Leitung notbetriebberechtigt ist. Falls mehrere Endgeräte angeschlossen sind, muss bei der Wahl S-Bus dann ein ISDN-Endgerät als Notbetriebsgerät konfiguriert werden. Das geht natürlich nur bei solchen Endgeräten, die den Notbetriebsmodus implementiert haben. Der Grund dafür: Im Notbetrieb darf nur mit einem ISDN-Endgerät telefoniert werden, da sonst zuviel Strom (Leistung) vom Amt «abgezogen» wird. Im Notbetrieb sind nicht alle Merkmale verfügbar, aber zumindest kann telefoniert werden. Da heute beinahe in jedem Haushalt ein Mobiltelefon vorhanden ist, wird bei einem ISDN-Unterbruch wohl als erste Reaktion auf das Handy gewechselt.

Die IT-Sicherheit und -Verfügbarkeit hängt oft auch von der betrieblichen Organisation ab. Worauf setzt Swisscom bei der Sicherheits-Prozessorganisation?
Das Prozessnetzwerk von Swisscom Fixnet machte es mithilfe der zwei international anerkannten Standards BS7799(*) und der OSSTMM (Open Source Security Testing Methodologie Manual)-Methode möglich, die nötigen Prozesse und Instrumente aufzubauen. Der Sicherheit wird auf allen Organisationsebenen Rechnung getragen.
Die Operational Security von Swisscom Fixnet hat folgende Aufgaben:

- *Projekte:* Begleitung, Unterstützung und Review der Projekte während allen Projektephasen
- *Security Training und Consulting:* Ausbildung und Schulung von Sicherheitsprozessen und Abläufen inklusive Audits nach der OSSTMM-Methode in regelmässigen Abständen. Erarbeitung der operativen Sicherheitsrichtlinien und Unterstützung der betrieblichen und Engineering-Prozesse in Sicherheitsfragen, Initialisierung von Sicherheitsprojekten
- *Cockpit und Reporting:* Reporting an die Führung des Bereichs Security von Swisscom Fixnet für Systemkomplexe, Teilsysteme und Komponenten
- *Legal und Policies:* Abklärungen der Konformität mit dem Gesetz für Werk-, Wartungs- und Lieferantenverträge
- *Operation und Testing:* Testen bestehender und neuer OSS Hardware, Software und Netzwerkkomponenten nach den erarbeiteten Methoden (Nessus Attacken usw.), rekursives Härten bzw. Optimieren der OSS-Plattformen, Netzwerke und Systeme nach Bekannt werden neuer Sicherheitslücken (Exploits), Anpassung der Regelwerke um Exploits abzuwehren

Die Sicherheitsmessung ist für die Risikoanalyse eine grosse Herausforderung. Welche Instrumente sind hier viel versprechend?
Bei Swisscom Fixnet wurde eigens eine Organisationseinheit zur Bemessung der operativen IT-Sicherheit ins Leben gerufen. Es liegt in der Verantwortung dieser Unit, die operative Umsetzung der strategischen Richtlinien und Vorgaben zu bemessen und zu erzeugen. Ein Kernanliegen war einerseits, ein komplettes und skalierbares, gleichzeitig aber auch flexibles Sicherheits-Management-Framework aufzubauen.

Speziell dafür eingerichtete Anlagen unterziehen die bestehenden Infrastrukturen zyklisch standardisierten Sicherheits-Audits. Die Landschaft wird in den Bereichen Design, Implementation und Operation auf die Einhaltung der Vorgaben fortlaufend bemessen. Veränderungen oder Bedrohungen werden so frühzeitig wahrgenommen und Schadensereignisse aktiv antizipiert. Die Resultate dieser Sicherheitstests dienen als Grundlage zur Berechnung des Risk Assessment Values (RAV). Der RAV-Wert ist die Sicherheitskennzahl der OSSTMM-Methode und repräsentiert die gemessene Sicherheit (Anzahl der Verwundbarkeiten, Schwächen, Bedenken usw.). Diese Kennzahl ermöglicht eine aktive Steuerung des Sicherheitsniveaus in allen Bereichen. Anhand des beschlossenen Sicherheitsniveaus wird der Handlungsbedarf klar und faktisch in jedem Bereich aufgezeigt. Das Risk Assessment (Eintrittswahrscheinlichkeit multipliziert mit dem Schadensausmass) wird damit um eine Dimension erweitert und erhält eine direkte Schnittstelle zu der Infrastruktur bzw. den Messungen und Resultaten von OSSTMM.

Kontrolle und Benchmark für die Sicherheitsstandards der Firma werden heute auch über Sicherheitszertifikate erworben. Setzt Swisscom auf das deutsche BSI-Zetrifikat oder auf den britischen Standard 7799-1?
Swisscom Fixnet AG arbeitet nach dem britischen ITIL-Standard und demzufolge auch nach dem britischen Information Security Standard BS7799/ISO17799. Ein Zertifizierung bezüglich BS7799 wird aktuell noch nicht angestrebt, wird aber in den nächsten Monaten geprüft.

Unter dem Begriff Sicherheitskultur werden Mitarbeiter fortlaufend auf die Technik sensibilisiert. Swisscom war in diesem Bereich Pionier. Wie hat sich die Sicherheitskultur entwickelt?
Bei Swisscom Fixnet wurde in den Jahren 2003/04 eine Sensibilisierungskampagne zum Thema Informationssicherheit durchgeführt, und dies von der Geschäftsleitung bis hin zu jedem Mitarbeiter. Insgesamt haben über 7500 Mitarbeitende je einen Workshop mit einer Dauer von rund einer Stunde durch den jeweiligen Vorgesetzten erhalten. Dieser Workshop enthielt eine Präsentation, ein Video sowie ein selbst bestimmter Massnahmenkatalog «Was müssen wir unbedingt verbessern?». Zusätzlich wurden den Mitarbeitenden Broschüren und Plakate mit den angestrebten Verhaltensregeln ausgehändigt, sowie Messungen und Analysen anhand von Audits durchgeführt. Um das damit erzielte Sicherheitsbewusstsein aufrecht zu erhalten, braucht es jedoch nach rund ein bis zwei Jahren ein Refreshing. ■


ERICSSON
TAKING YOU FORWARD
SAY THIS IS YOUR COMPANY TRYING TO GET TO THE NEXT LEVEL
AND THIS IS THE TECHNOLOGY THAT WILL HELP YOU
WELL THIS IS US MAKING SURE YOU CAN TRUST THE TECHNOLOGY
To take the next big step, your business needs technology it can rely on. So let's talk. Ericsson invest more in R&D than anyone else in the telecoms industry. We support over 450 networks in over 140 countries; fixed and mobile, via all the 3G technologies. And we've the capacity to manage and evolve your network every step of the way. Which lets you concentrate on getting to the top.
www.ericsson.com