CoreTEC
IT Security Solutions GmbH

Network-Security für Internet Provider

Christian Mock
CoreTEC IT Security Solutions GmbH
cm@coretec.at
www.coretec.at

CoreTEC IT Security Solutions GmbH

Inhalt

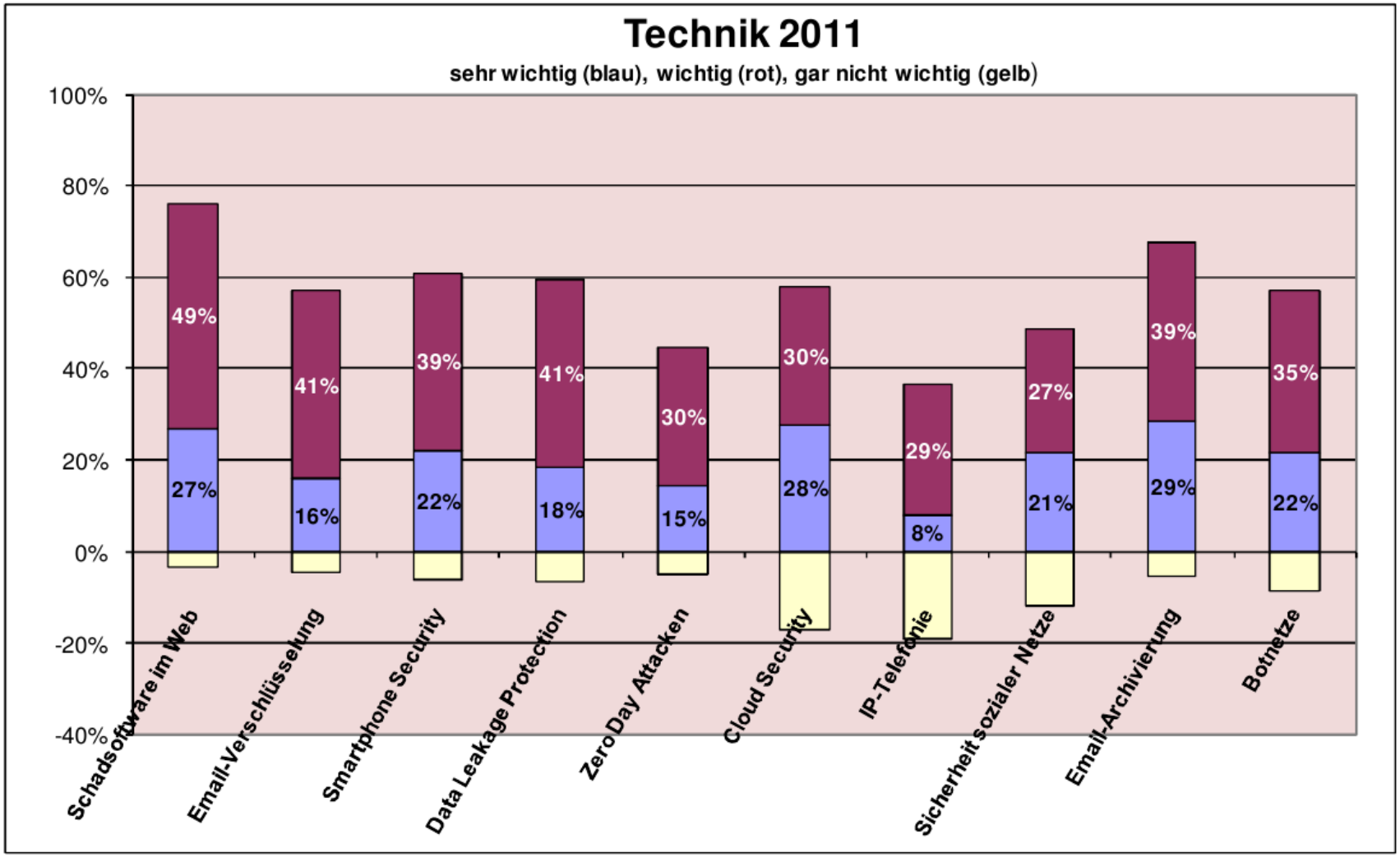
- Aktuelle Security-Entwicklungen
- Wo drückt den Kunden der Schuh?
- Mögliche Lösungen vom Provider
- Standard-Securitymaßnahmen
- Dies und das

Über mich

- 1994 einer der Gründer von PING
- Security hauptberuflich seit 1997
- 2001 einer der Gründer von CoreTEC
- Schwerpunkt auf komplexen Lösungen, Penetration Testing, technisches Consulting
- Kunden: KMUs, große Unternehmen
- Mitarbeit bei CIRCA, Domainbeirat

CoreTEC IT Security Solutions GmbH

Security-Themen 2011



http://www.eco.de/dokumente/eco_Umfrage_Sicherheit_2011

Malware aus dem Web

- Die Zeit der Email-Viren ist vorbei
- Drive-By-Downloads sind angesagt
- Direktes Problem für ISP: Zombies
  - was das bedeutet, brauch ich ja hier nicht erklären
- Technische Lösungen gibt's zuhauf
  - Virenscanner, Content-Scanner-Gateways, tlw. in Firewalls integriert (“UTM” - Unified Threat Management)
- Kann der ISP was tun, was politisch ungefährlich ist?
  - siehe Tunesien und Facebook
  - immer ein Eingriff in Web-Verkehr → Vorratsdatenspeicherung

Smartphone-Security

- Für mich ist hier momentan nur das Problem bekannt, keine Lösungsansätze sichtbar
  - Selber Administrations-Sauhaufen wie am Beginn der PC-Ära, aber Internet-Enabled und immer dabei (=leicht verloren)
- Die sexy Smartphones haben nichteinmal brauchbare Funktionen zur zentralen Administration
  - Sperrung/Datenlöschung bei Verlust? 3rd Party-Lösungen
  - Backup? Nicht ohne root!
  - Kontrolle der installierten Apps? Nix.
  - Vertrauen in Apples App-Auswahl und Androids Permissions?
  - Bleibt nur der Blackberry...

Data Leakage Prevention

- Buzzword, Wikileaks als Schreckgespenst
- “Wie verhindere ich, daß meine schützenswerten Firmendaten fremdgehen?”
- Was kann der Provider tun?
  - Müßte gesamten Datenverkehr (zumindest Mail, WWW, ftp) scannen
  - Dann fehlt noch Kontrolle über USB-Ports, DVD-Brenner, Drucker...
  - Evtl sinnvoll bei ASPs

Cloud Security

- Bitte definieren Sie “Cloud”...
- In Sachen ASP/SaaS:
  - Stehlen von Credentials (Phishing, Reuse von Paßwörtern für mehrere Sites...)
  - Bugs in der Software → Überspringen von Mandantengrenzen
  - Beides ist im klassischen Modell kein (so großes) Problem
  - Wo läuft das physisch? Jurisdiktion!
- Wie gewinne und verdiene ich das Vertrauen?
  - Strong Authentication (2 Faktor, siehe gmail)
  - Technische Maßnahmen: Secure Coding, Penetration Tests
  - Organisatorisch: ISO 27001 (see below...)

IP-Telefonie

- Dictionary-Attacks auf SIP-Accounts ohne Ende
  - 3-4 Angriffe/Tag auf eine kleine Asterisk-Installation
  - Berichte über tausende EUR Schäden in einer Nacht
- Hosted PBX:
  - Starke Default-Paßwörter, Paßwort-Policies
  - Usage-Monitoring/Kostenobergrenzen
- Beratung der Kunden
- Gibt's Erfahrungen über sonstige Angriffe?
  - Abhören
  - Calls rerouten

Da fehlt doch was...

- IPv6? Hallo, aufwachen, liebe Kunden!
- Kaum einer kennt sich aus
- Implementationen unreif/wenig getestet
  - Auch 2011 bei Security-Herstellern noch Stiefkind
- Vogel-Strauß-Politik bei Kunden
  - Außerdem haben's auch ohne v6-Einführung schon zuwenig Leute und Budget
- Da wird's noch gewaltig krachen

Große Kunden...

- Machen sich die Security selber, brauchen sie nur dort vom ISP, wo sie selber nicht können...
- Connectivity-Provider
  - Verfügbarkeit/Redundanz
  - Schutz gegen DDoS
  - Schnelle Erreichbarkeit bei Problemen
- Hosting-Provider
  - Physische Sicherheit
  - evtl 27001-Zertifizierung (see below)

Kleine Kunden...

- Know-How/Manpower für eigene Security fehlt
- Brauchen Lösungen für
  - Firewall
  - Malware-Scan (Mail, Web)
  - günstige redundante Connectivity (UMTS)
  - Content-Filter für Facebook, Youtube, Skype...
  - Offsite-Backup
  - ...
- Hier gibt's definitiv Business-Potential

Managed Security Services

- Kunde kauft Firewall-Appliance
  - Anschaffungskosten + Setup-Fee
  - “UTM”, dh. inkl. Virenscan, Content-Filter, IPS...
- Zentrales, mandantenfähiges Management
- Konfiguration inkl. Beratung als Fair Use-Modell
  - 99,- monatlich
  - “inkludiert alles, wo wir unser Büro nicht verlassen müssen”
- Kann man abkupfern oder in Kooperation mit uns machen :-)

</Werbeeinschaltung>

Security für den Provider

- Was kann der Provider in seinem Netz tun?
- Ingress/Egress Filtering
  - Wer hat's umgesetzt?
  - RFC2827 wär aus 2000
  - Bringt einem selber nicht viel, aber dem Rest des Netzes gg DDoS
- Erkennen und Blocken von Zombies
  - Erfahrungen?

Security für den Provider

- Firewall vor die Server
  - Performancemäßig kein Thema
  - Wieviel Vorfälle gibt's, wo das was brächte? (SMTP, HTTP, … muß eh für die Welt offen sein)
- IDS/IPS (für die Server)
  - Wieder: bringt's was?
- Management des Equipments
  - eigenes Management-Netz vorhanden?
  - dann kann ich ssh, https auf dem public IF abdrehen
  - und wie steht's mit Security-Updates/Patches?

Security für den Provider

- Authentisierung der Admins/Mitarbeiter
  - 2 Faktor?
  - Policies?
  - Aufräumen von Alt-Accounts?
  - Schon mal Social Engineering versucht?
- Authentisierung der Kunden am System und Helpdesk
  - Gmail macht (optional) 2 Faktor
  - Social Engineering gegen Helpdesk...

Services für den Kunden

- Bietet eigentlich irgendwer die Standard-Services ausschließlich über SSL an?
  - SMTP, POP
  - Kundenportal
  - Webserver-Upload
- Konfiguration der CPE
  - Default-Admin-Paßwort (Telekom, Pirelli)
  - Verschlüsselung des WLANs
- Webmail-Virenscan: wenn, dann richtig
  - wenn man ein Draft mit Attachment ohne Scan speichern und downloaden kann, ist's falsch...

Web Application Firewalls

- Schützt den Webserver, macht nur HTTP(S)/HTML
- Nicht nur Pattern-basiert, auch generische Schutzmechanismen
- Angesichts der traurigen Qualität von Webapp-Code sehr empfehlenswert
- **Aaaber:** sehr aufwendig zu integrieren
  - Muß auf die jeweilige App angepaßt werden
  - Evtl muß die App angepaßt werden, um vollen Schutz zu haben
- Eher was für dedicated ASPs

ISO27001

- Norm über Informationssicherheits-Managementsysteme, quasi ISO9000 für InfoSec
- langsamer Trend für Firmen-Rechenzentren, sich zertifizieren zu lassen
- Outsourcing-Partner tun sich leichter, wenn sie auch zertifiziert sind
  - geht auch ohne, dann halt wasserdichte SLAs etc.
- Für Hosting-Provider/ASPs evtl interessant

Dies und das

- Schon mal versucht, der Polizei einen versuchten Internet-Betrug zu melden?
  - muß am lokalen Wachzimmer passieren, viel Spaß!
  - Generell wenig Info verfügbar über Vorgehensweisen
  - Wär eine Aufgabe für die ISPA...
- Wie schütz ich eigentlich die vorratsgespeicherten Daten?
  - Wenn's denn einmal kommt
  - Schadenspotential groß, weil Datenbestand groß und Zentral