
österreichische
LOTTERIEN
CASINOS AUSTRIA
Machen Sie Ihr Spiel
Konzernweite
Mailverschlüsselung

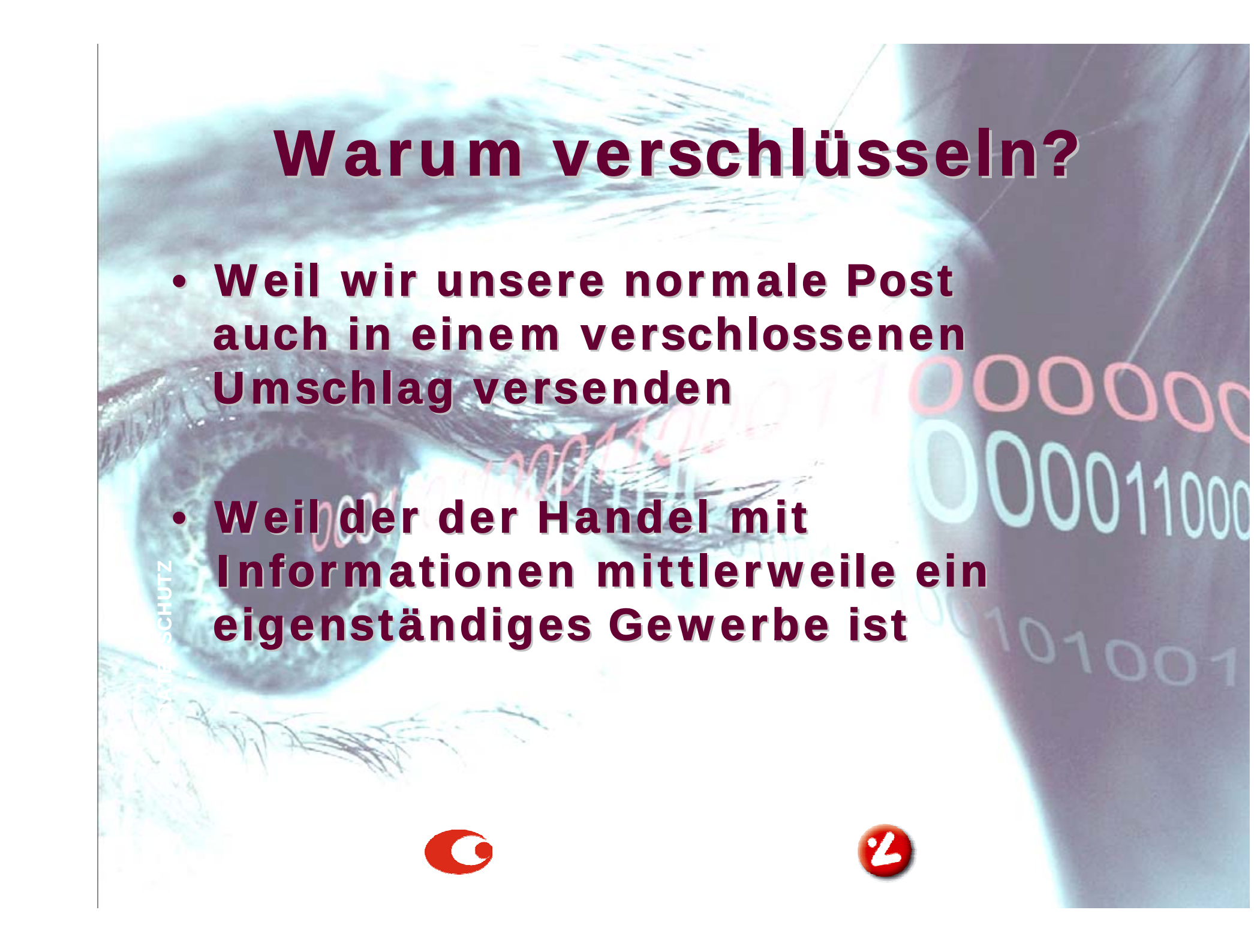
Agenda

- Warum eigentlich Mailverschlüsselung?
- Schwächen der „üblichen“ Workarounds
- Umsetzung
  - Schematische Übersicht
  - Benötigte Komponenten
  - Aufwand bei der Implementierung
  - Kostenschätzung
- Aufwand im Betrieb
- Es geht noch cleverer
- Konklusio

Warum verschlüsseln?

- Weil wir unsere normale Post auch in einem verschlossenen Umschlag versenden

- Weil der der Handel mit Informationen mittlerweile ein eigenständiges Gewerbe ist



Warum Mailverschlüsselung?

- Vermehrter Bedarf bei Casinos Austria International sowie bei einigen ÖLG Mitarbeitern (Datenaustausch mit ausländischen Tochterfirmen, sensible Korrespondenz)

- Früher wurden teils wirklich sensible Informationen für alle gut lesbar „auf Postkarten“ ausgetauscht

Die „üblichen“ Workarounds

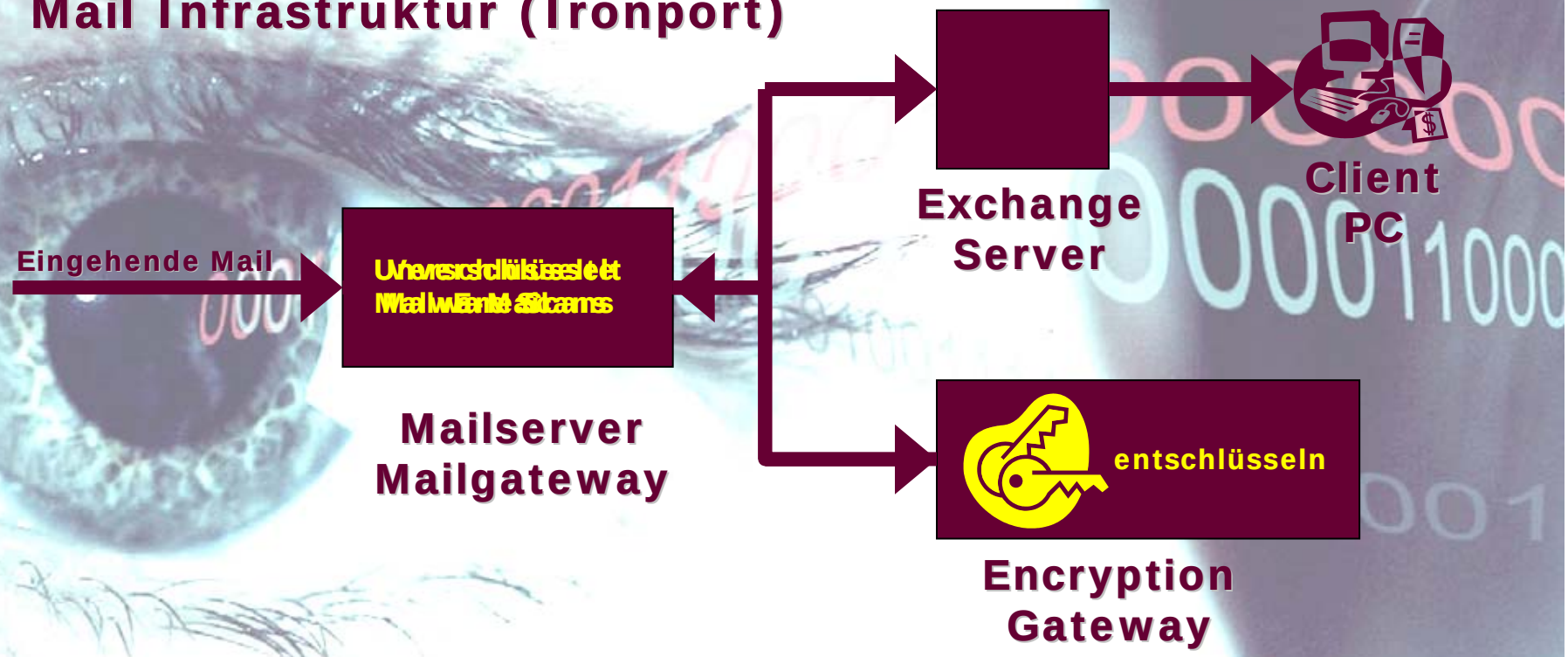
- Lokal installiertes PGP ist für den Anwender sehr schwer zu handhaben
  - dadurch große Akzeptanzprobleme bei den Anwendern
  - dadurch Nutzung nur wenn „unbedingt“ erforderlich
- Der Workaround „verschlüsseltes ZIP-File“ ist oftmals kontraproduktiv
  - „falsch“ verschlüsselte ZIP-Files sind binnen Minuten gecrackt
  - Wie wird das Passwort zum ZIP-File sicher ausgetauscht
- Verschlüsselte E-Mails können erst am Client auf Malware untersucht werden

Die „üblichen“ Workarounds

- Gefahr von Datenverlust
  - Verliert der Anwender seinen Private Key können verschlüsselte E-Mails nicht mehr gelesen werden
- Problem bei der Archivierung
  - Bei individuell verschlüsselten E-Mails ist es fast unmöglich sicherzustellen, dass diese auch wirklich in Zukunft zurückgesichert werden können.
- Keine Perimeter Security
  - Erst am Client kann überprüft werden ob die E-Mail Malware enthält
- Langfristig zu teurer
  - Einzellizenzen, sehr großer Betreuungsaufwand

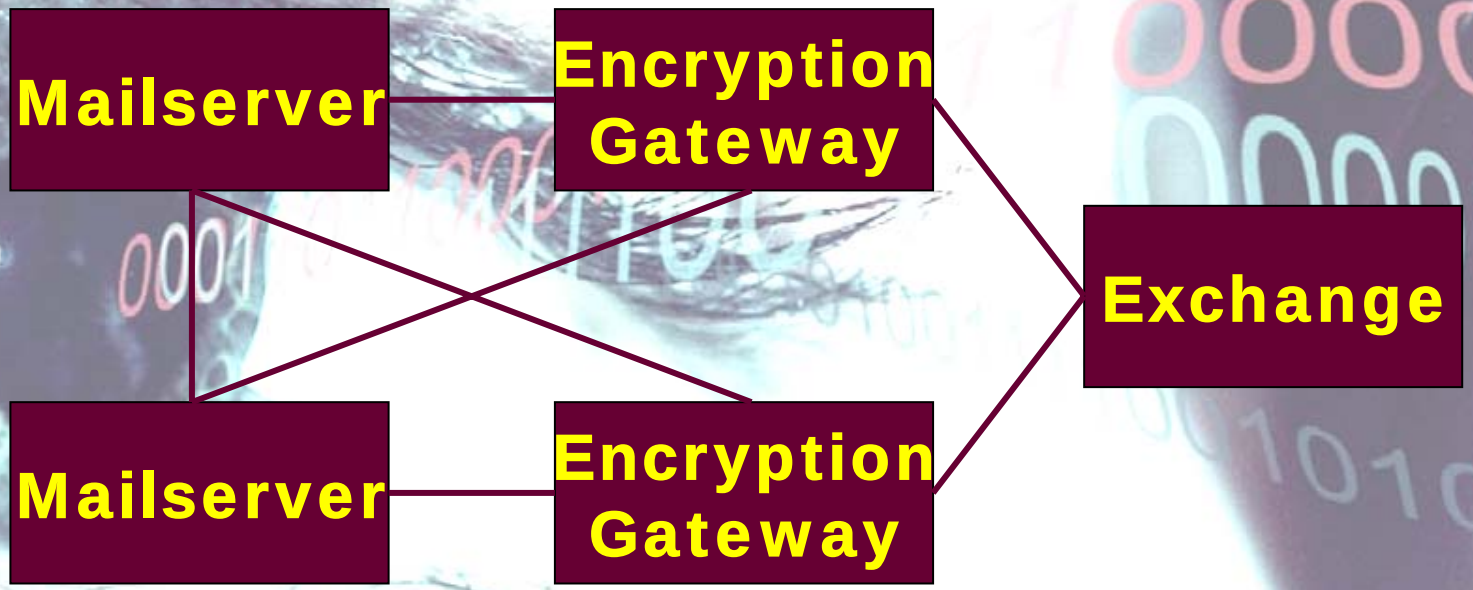
Umsetzung / Schematische Übersicht

Migration in die vorhandene Mail Infrastruktur (Ironport)



Umsetzung / Schematische Übersicht

Redundanz ist natürlich möglich!



Quick Wins

- Ablöse der PGP Lösung zwischen ÖLG und verschiedenen Klassenlotterieanbietern
- Absicherung der Kommunikation zwischen dem Unternehmen und Unternehmensberatern

Umsetzung / Benötigte Komponenten

- **Am Client: Keinerlei Eingriffe notwendig!**
- **Serverseitig: Windows 2000/2003 oder Linux oder Sun**
  Mind. 1GHz / 512Mb

Plattformunabhängig weil in JAVA entwickelt

Aufwand bei der Implementierung

- **Planung intern 14 Manntage**
  - **Erstellung von Manuals für Enduser und externe Mailparter, Recherche wer ad-hoc Mailverschlüsselung einsetzen muß**
- **Umsetzung intern 5 Manntage**
  - **ohne Hardware- und Basissetup**
- **Zwei Manntage Consulting durch den Hersteller**

Aufwand im Betrieb

- 1 Stunde pro neu anzulegendem User
  - Erstellung des digitalen Zertifikats auf www.a-cert.at
  - Einrichten des Users auf dem Mail- und Verschlüsselungsgateway
  - Kommunikation mit dem externen Mailpartner (Übermittlung des Rootzertifikats)
- 1 Manntag pro Monat für Updates, Troubleshooting etc.

Kosten

- **Kosten für Hardware- und Basisplattform**
  - **Windows, Linux, Solaris**

- **Kosten für die Software*:**
  - **für 20 Arbeitsplätze** **€ 1.340,-**
  - **für 50 Arbeitsplätze** **€ 2.750,-**
  - **für 100 Arbeitsplätze** **€ 4.600,-**
  - **für 200 Arbeitsplätze** **€ 7.800,-**

*** Listenpreise netto unverhandelt**

Es geht noch cleverer

- TLS Verschlüsselung zwischen Mailservern sorgt für sichere Kommunikation sämtlicher Anwender der betroffenen Unternehmen
- Wird von praktisch jedem bekannten Mailserver unterstützt

Es geht noch cleverer

- Ende-zu-Ende-Verschlüsselung mittels symmetrischer Algorithmen.
- Der verwendete Schlüssel wird im Voraus über ein weiteres Protokoll (z. B. das SSL Handshake Protocol) ausgehandelt und ist einmalig für die Verbindung.

Es geht noch cleverer

- Kosten nahezu = 0 da lediglich ein Zertifikat pro Mailserver benötigt wird
- Noch weniger (kein) Aufwand für den Endanwender als bei SMIME Gateway, dadurch 100% Akzeptanz ☺

Konklusio

- Mit einer Lösung wird das gesamte Spektrum der Anforderungen (noch) nicht abgedeckt
- TLS Server <–> Server Verschlüsselung wäre am idealsten (wenn alle anderen mitmachen würden)

Danke für Ihre Aufmerksamkeit!

michael.mrak@casinos.at
0664 / 5032331