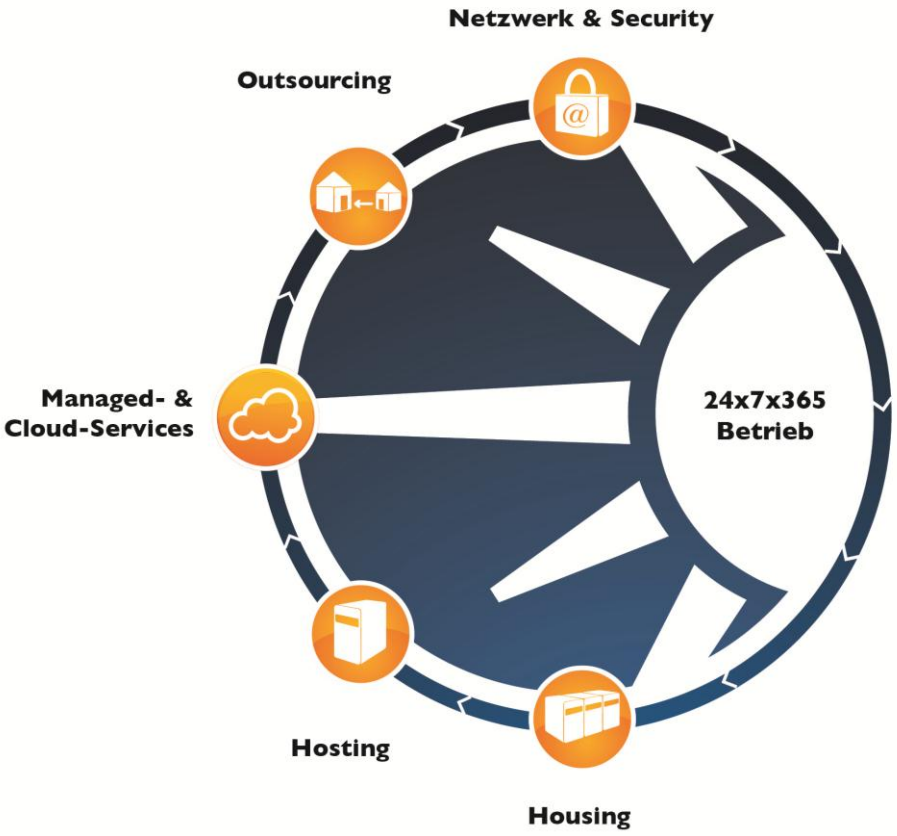
Die ganze Wahrheit über Hackingangriffe?
Motive und Auswirkungen

Daten nützen | Daten schützen



Gerhard Haider
CEO

Mail: g.haider@conova.com
Mobil: +43 (0)676 830 50 500

Hackingangriff?

- **50% aller Unternehmen wurden bereits gehackt!**
- **Die anderen 50% der Unternehmen wissen nicht, dass sie bereits gehackt wurden!**

Fortune 500:

Rang	Name	Hauptsitz	Land
1.	Royal Dutch Shell	Den Haag	Niederlande
2.	ExxonMobil	Irving	USA
3.	Walmart	Bentonville	USA
4.	BP	London	Großbritannien
5.	Sinopec	Peking	China
6.	China National Petroleum	Peking	China
7.	State Grid	Peking	
8.	Chevron	San Ramon	
9.	ConocoPhillips	Houston	
10.	Toyota Motor	Toyota	

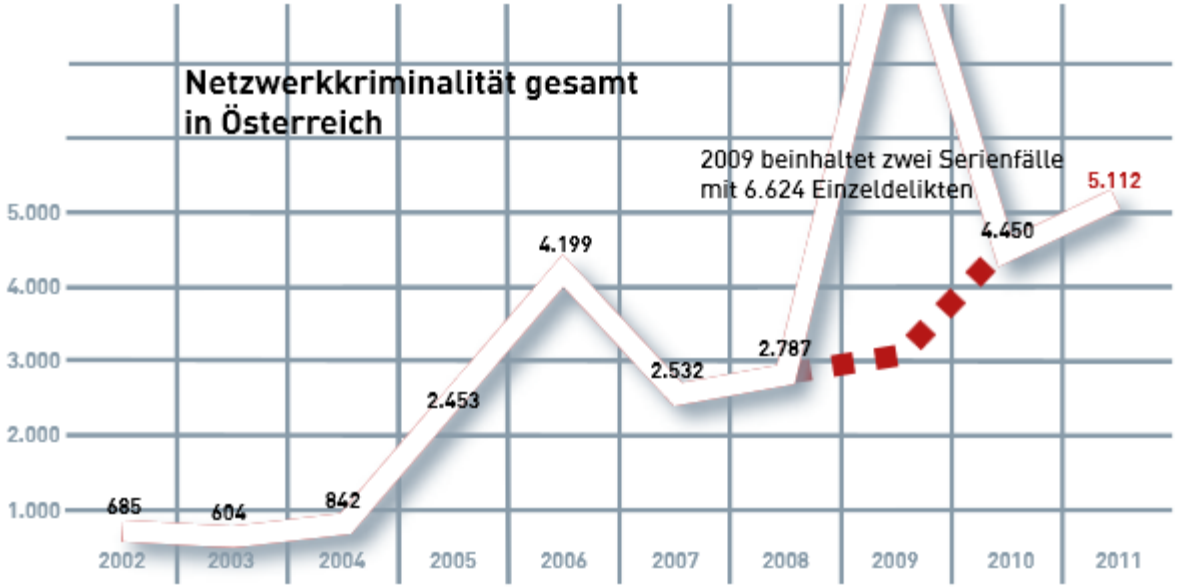
Interbrand					
Platz[18]		Marke	Markenwert [Mrd US-$]	Ursprung	Veränderung in Prozent
	1	Coca-Cola	77,839	USA	+ 8
▲	2	Apple	76,568	USA	+129
▼	3	IBM	75,532	USA	+ 8
	4	Google	69,726	USA	+26
▼	5	Microsoft	57,853	USA	− 2
▼	6	General Electric	43,682	USA	+ 2
▼	7	McDonald's	40,062	USA	+13
▼	8	Intel	39,385	USA	+12
▲	9	Samsung	32,893	Südkorea	+40
▲	10	Toyota	30,280	Japan	+ 9

Quelle: http://de.wikipedia.org/wiki/Liste_der_gr%C3%B6%C3%9Ften_Unternehmen_der_Welt

Ziele

1. Aufzeigen der Auswirkungen eines Hackingangriffes
2. Vermitteln, dass Hackingangriffe kein Kavaliersdelikt sind!
3. Vorbeugen ist besser als Heilen!
4. Vorbereitung Notfallplan

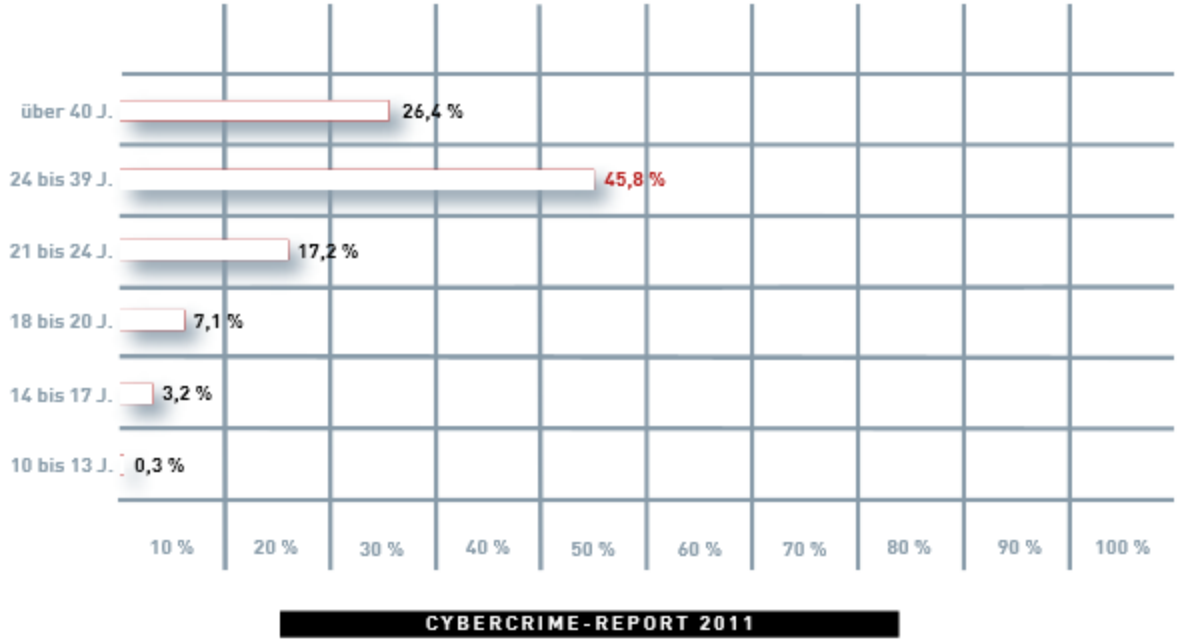
Bundeskriminalamt



- Die Aufklärungsquote lag 2011 durchschnittlich bei 43,7 Prozent!

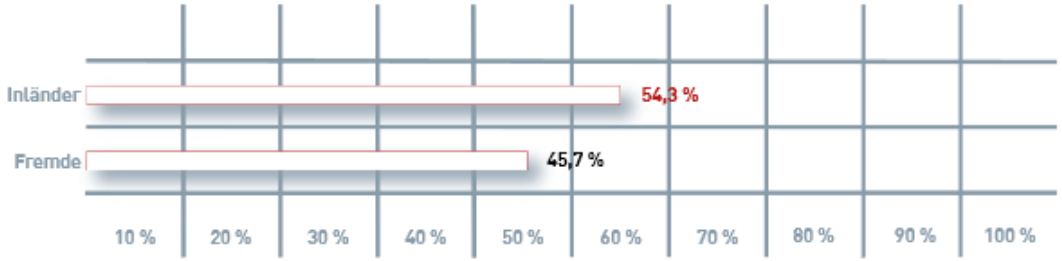
Quelle: http://www.bmi.gv.at/cms/BK/publikationen/files/CybercrimeReport2011web.pdf

Bundeskriminalamt

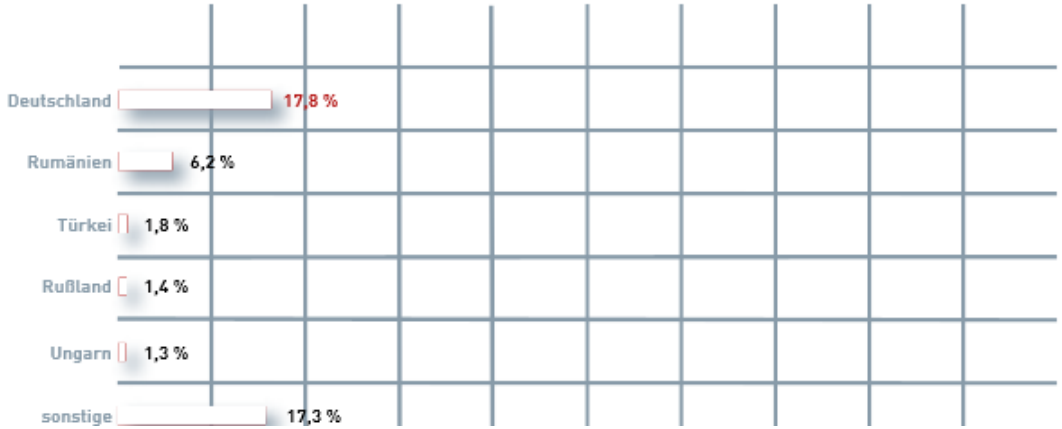


Quelle: http://www.bmi.gv.at/cms/BK/publikationen/files/CybercrimeReport2011web.pdf

Bundeskriminalamt



Der Anteil an Nicht-Österreicherinnen und Nicht-Österreichern beträgt rund 46 Prozent, wobei Deutschland mit rund 18 Prozent und Rumänien mit rund sechs Prozent den größten Anteil stellen. Hier wirkt sich die räumliche und sprachliche Nähe zu Deutschland, vor allem bei den Betrugsfällen im Internet, aus. Ansonsten ist schwerpunktmäßig eine Verteilung der Täter im osteuropäischen Raum zu erkennen.



Quelle: http://www.bmi.gv.at/cms/BK/publikationen/files/CybercrimeReport2011web.pdf

conova communications GmbH
+43 (0)662 22 00 - 334
sales@conova.com | www.conova.com

Zentrale Salzburg: Karolingerstraße 36A | 5020 Salzburg | Tel: +43 (0)662 22 00 - 0 | Fax: +43 (0)662 22 00 - 209
Büro Wien/Schwechat: Wiener Straße 30/02 | 2320 Schwechat | Tel: +43 (0)662 22 00 - 0 | Fax: +43 (0)662 22 00 - 409
Offenlegung nach § 14 UGB: Rechtsform: GmbH | Sitz: Salzburg | FN: FN64293z | DVR: 9125419 | Firmenbuchgericht: Landesgericht Salzburg

Einbruch versus Hackingangriff

1. Einbrecher
    1. Tür wird aufgebrochen
    2. Haus wird durchsucht
    3. Wertgegenstände werden mitgenommen
    4. Strafbar?

2. Hacker /Cracker
    1. „Tür“ wird aufgebrochen
    2. „Haus“ wird durchsucht
    3. „Wertgegenstände“ werden mitgenommen
    4. Strafbar?
3. Hacker versus Cracker
    1. Hackers build things, crackers break them
    2. Vielen Dank für den Hinweis, dass es möglich war, meine Türe aufzubrechen!

Motive eines Hackers

1. „Challenge“
2. Nicht zwingend die Absicht zu zerstören
3. Anerkennung

Rechtlicher Rahmen

Widerrechtlicher Zugriff auf ein Computersystem

§ 118a. (1) Wer sich in der Absicht, sich oder einem anderen Unbefugten von in einem Computersystem gespeicherten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, **dass er die Daten selbst benützt**, **einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht**, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen Zugang verschafft, indem er spezifische Sicherheitsvorkehrungen im Computersystem überwindet, ist mit Freiheitsstrafe bis zu **sechs Monaten** oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.
(2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.
(3) Wer die Tat als **Mitglied einer kriminellen Vereinigung** begeht, ist mit Freiheitsstrafe bis zu **drei Jahren** zu bestrafen.

Datenbeschädigung

§ 126a. (1) Wer einen anderen dadurch schädigt, daß er automationsunterstützt verarbeitete, übermittelte oder überlassene Daten, über die er nicht oder nicht allein verfügen darf, **verändert, löscht oder sonst unbrauchbar macht** oder unterdrückt, ist mit Freiheitsstrafe bis zu **sechs Monaten** oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.
(2) Wer durch die Tat an den Daten einen 3 000 Euro übersteigenden Schaden herbeiführt, ist mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bis zu 360 Tagessätzen, wer einen 50 000 Euro übersteigenden Schaden herbeiführt oder die Tat als **Mitglied einer kriminellen Vereinigung** begeht, mit Freiheitsstrafe von sechs Monaten bis zu **fünf Jahren** zu bestrafen.

Störung der Funktionsfähigkeit eines Computersystems

§ 126b. (1) Wer die Funktionsfähigkeit eines Computersystems, über das er nicht oder nicht allein verfügen darf, dadurch schwer stört, dass er Daten eingibt oder übermittelt, ist, wenn die Tat nicht nach § 126a mit Strafe bedroht ist, mit Freiheitsstrafe bis zu **sechs Monaten** oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Rechtlicher Rahmen

(2) Wer durch die Tat eine längere Zeit andauernde Störung der Funktionsfähigkeit eines Computersystems herbeiführt, ist mit Freiheitsstrafe bis zu **zwei Jahren** oder mit Geldstrafe bis zu 360 Tagessätzen, wer die Tat als **Mitglied einer kriminellen Vereinigung** begeht, mit Freiheitsstrafe von sechs Monaten bis zu **fünf Jahren** zu bestrafen.

Missbrauch von Computerprogrammen oder Zugangsdaten

§ 126c. (1) Wer

1. ein Computerprogramm, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a), einer Verletzung des Telekommunikationsgeheimnisses (§ 119), eines missbräuchlichen Abfangens von Daten (§ 119a), einer Datenbeschädigung (§ 126a), einer Störung der Funktionsfähigkeit eines Computersystems (§ 126b) oder eines betrügerischen Datenverarbeitungsmissbrauchs (§ 148a) geschaffen oder adaptiert worden ist, oder eine vergleichbare solche Vorrichtung oder
2. ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen,

mit dem Vorsatz herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht, sich verschafft oder besitzt, dass sie zur Begehung einer der in Z 1 genannten strafbaren Handlungen gebraucht werden, ist mit Freiheitsstrafe bis zu **sechs Monaten** oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Nach Abs. 1 ist nicht zu bestrafen, wer freiwillig verhindert, dass das in Abs. 1 genannte Computerprogramm oder die damit vergleichbare Vorrichtung oder das Passwort, der Zugangscode oder die damit vergleichbaren Daten in der in den §§ 118a, 119, 119a, 126a, 126b oder 148a bezeichneten Weise gebraucht werden. Besteht die Gefahr eines solchen Gebrauches nicht oder ist sie ohne Zutun des Täters beseitigt worden, so ist er nicht zu bestrafen, wenn er sich in Unkenntnis dessen freiwillig und ernstlich bemüht, sie zu beseitigen.

Salzburger Rechenzentrum gehackt

Von Sn | 11.12.2012 - 16:08 | Kommentieren

Das Salzburger Rechenzentrum der conova communications GmbH ist trotz hoher Sicherheitsvorkehrungen Opfer eines Hackerangriffs geworden. Dabei wurden auch Zugangsdaten von Kunden der conova-Server entwendet.

- Generell: > 100 Hackingangriffe/ Attacken täglich, welche erfolgreich abgewehrt werden

- 2.12.2012 Kenntnis, dass Zugangsdaten unseres Mail- und Webhostverwaltungssystems entwendet wurden!

Mögliche Auswirkungen

- Generell:
  - Zentrale Verwaltungs- und Administrationsplattform für Mails und Webhosts
  - Mehrere Tausend Kunden
  - Primär Privatkunden, aber auch KMUs

- Mitlesen von Mails möglich
- Änderung von Inhalten der Website (Shop, ..)
- Änderung der Zugangsdaten und Aussperren des Benutzers möglich

Unser Ziel

- Kundeninfo?
- Verhinderung, dass Website‘s der Kunden verunstaltet werden
- Verhinderung, dass Zugangsdaten (Mail, Web) geändert werden
- Cracker von unserer Information/Kommunikation mit Kunden aussperren
- Kunden wieder volle Möglichkeiten geben, sobald Feature aktiv
- Raschest mögliche Umsetzung um Hacker das Mitlesen von Mails nicht zu ermöglichen
- Zuerst alle Kunden direkt informieren, dann Presse
- Presseaussendungstermin wurde mit 11.12.2012 um 14.30 festgelegt

Technik

- Programmierung einer Funktion, dass in unserer Verwaltungsplattform neben Username und Passwort ein weiteres Authentifizierungsmerkmal benötigt wird → AuthCode
- Zeit bis 08.12.2013

Kommunikation

- Informationsbrief an Kunden mit Authentication Code →09.12.2012
  - Print
  - Kuvertierung
- Pressemeldung → 10.12.2012
- Q&A für Mitarbeiter im Falle von Kundenrückfragen → 10.12.2012
- Website-Info → 10.12.2012
- Social media → 10.12.2012
- Versand 10.12.2012 07:00
- Faxversand 11.12.2012
- Bearbeitung der Onlineforeneinträge
- Beantwortung von konkreten Kundenanfragen

Begleitende Timeline

- 3.12.2012
  - Krisenteam definieren
  - Kontaktaufnahme Kripo
  - Start der technischen Aktivitäten
  - Kundeninformation?
- 4.12.2012
  - Einbindung Krisenagentur
  - Start der Entwicklung des Features „Authcode“
- 05.-10.12.2012
  - Klärung Versand / Mailingagentur / Fax
  - Vorbereitung Pressetexte, Kundentexte, Website, Facebook
  - Vorbereitung Mitarbeiterinfos
  - Schulungen Helpdesk
  - Druck, Kuvertierung,……
  - Analyse der Angriffe
  - Minutiös geplante ToDo Liste

Begleitende Timeline

- 10.12.2012

  Aussendung der Authentication Codes per Post und Fax,

- 11.12.2012

  Start persönliche Infos an Kunden

  Presseaussendung

Kosten

- 3500 Technikerstunden
- Ca. 500 Administrationsstunden
- Kosten Krisenagentur
- Versand, etc…
- Kosten > ¼ Mio €

Empfehlungen / Erkenntnisse

- Es gibt keine 100%ige Sicherheit im Internet!
- Sicherheit hat immer Priorität!
- Erhöhung der Sicherheit günstiger, als Beseitigung der Schäden!
- Es kann auch „mir“ passieren
- Rechtzeitig auf ein WorstCase Szenario vorbereiten
- Hacking / Cracking ist krimineller Akt, welcher hohen Schaden bei betroffenen Unternehmen verursacht!

Gerhard Haider
CEO

Mail: g.haider@conova.com