# BERICHT INTERNET-SICHERHEIT ÖSTERREICH 2010

GovCERT AUSTRIA

CERT.at

# VORWORT

Staatssekretär
Dr. Josef Ostermayer

Die modernen Informations- und Kommunikationstechnologien (IKT) haben die Welt in einem vergleichbaren Ausmaß verändert wie die industrielle Revolution im 19. Jahrhundert. Sie beeinflussen immer mehr die Art, wie Unternehmen arbeiten, wie an Schulen gelehrt und gelernt wird, wie Behörden ihre Leistungen erbringen.

Auf dem Treffen des Europäischen Rats in Lissabon kamen die Staats- und Regierungschefs der Europäischen Union zu dem Schluss, dass auch Europa weitaus stärker zu einer digitalen Wirtschaft ausgebaut werden muss. Sie setzten der EU das Ziel, zum wettbewerbsfähigsten, wissensgestützten Wirtschaftsraum der Welt zu werden, indem vor allem das Internet und die Computertechnik als Motoren für Wirtschaftswachstum gefördert werden.
Je abhängiger wir alle von den IKT werden, umso mehr gewinnen jedoch deren Sicherheit und Zuverlässigkeit an Bedeutung. Schlagworte wie Spam, Computer-Viren, Phishing, Diebstahl elektronischer Identitäten stehen mit zunehmender Häufigkeit im Mittelpunkt einschlägiger Nachrichten. Im April 2007 ging der nahezu zweiwöchige "Cyber-Angriff" gegen Estland durch die Weltpresse, als nicht nur Regierungs- und Verwaltungssysteme ausfielen, sondern auch die größte estnische Bank für zwei Tage ihren internationalen Zahlungsverkehr einstellen musste. Ebenso waren Krankenhäuser und Energieversorgungssysteme tagelang in Mitleidenschaft gezogen, und die Angriffe richteten sich sogar gegen sämtliche Notrufnummern des Landes.

Als Antwort auf Bedrohungen dieser Art arbeiten nationale Regierungen und internationale Organisationen seit Jahren an einem Katalog von Maßnahmen zum Schutz der sogenannten kritischen Infrastruktur-Einrichtungen, die als wesentlich für die Aufrechterhaltung einer funktionierenden Gesellschaft gesehen werden.

Zu diesen Maßnahmen zählt der Aufbau eines Computer Emergency Response Team (CERT), bestehend aus IKT-Fachleuten, die Unterstützung bei Sicherheitsvorfällen bieten und bei der Wiederaufnahme des Betriebes helfen. Eine solche Organisation kann sich auf die Unterstützung eines einzigen Unternehmens beschränken, oder auch auf einen größeren spezifischen Kundenkreis wie z.B. Universitäts-Rechnernetze. Das seit April 2008 bestehende CERT.at versteht sich als nationale Institution insbesondere für kleine und mittlere Unternehmen. Es operiert gleichzeitig gemeinsam mit dem Bundeskanzleramt als Government-CERT zur Bekämpfung bzw. Prävention von Sicherheitsvorfällen in der öffentlichen Verwaltung und im Bereich der kritischen Infrastrukturen.
Nach nunmehr zweijährigem Betrieb legen CERT.at und GovCERT ihren ersten Tätigkeits- und Erfahrungsbericht vor. Es ist ein Report zur Lage der Internet-Sicherheit in Österreich. Dieser Bericht soll jährlich einen Überblick zu Herausforderungen und Lösungen in diesem entscheidenden Feld der Sicherheit geben. Er ist auch als ein Beitrag zum Kapitel Sicherheit und Konsumentenschutz der "Österreichischen Internetdeklaration" vom Februar des Jahres 2010 zu verstehen. Ich hoffe, dass die Leserinnen und Leser das Dokument als nützlich und informativ beurteilen und auch kommentieren werden. Denn die Arbeit von CERT lebt vom Dialog, vom Austausch und von Erfahrungen. Schließlich geht es um ein bedeutendes gemeinsames Ziel: den Schutz der kritischen Informationsinfrastrukturen in Österreich.

Ein CERT für Österreich – was ist das, wofür braucht man das? Der Begriff stammt aus den späten 80er Jahren – in den USA wurde damals das erste Computer Emergency Response Team gegründet. CERTs sind mittlerweile auch in vielen europäischen Staaten tätig und bilden ein globales Netzwerk für den Schutz der kritischen Infrastrukturen insbesondere im IKT-Bereich. Über 100 Organisationen allein in der EU zählen dazu.

In der Mitteilung KOM(2009) 149 vom März 2009 über den Schutz kritischer Informations-Infrastrukturen schlägt die Europäische Kommission einen Aktionsplan vor, der unter anderem auch die Schaffung von nationalen CERTs/GovCERTs in allen EU-Mitgliedstaaten bis spätestens Ende 2011 vorsieht. Die "Digitale Agenda für Europa" vom Mai 2010 bekräftigt im Kapitel Vertrauen und Sicherheit nochmals die Bedeutung dieser Themen und schlägt entsprechende Aktionen vor.

In Österreich wurden auf Initiative des Bundeskanzleramtes und der Internet Foundation Austria (IPA) mit Unterstützung der Universität Wien im Jahr 2007 das CERT.at und das GovCERT.at als Public-Private-Partnership ins Leben gerufen. Anfang 2008 wurde der Betrieb aufgenommen. Mit der operativen Abwicklung wurden Spezialisten von nic.at beauftragt.

CERT.at und GovCERT fungieren gemeinsam als Drehscheibe für Sicherheit, als Frühwarnsystem und Koordinierungsstelle für den Schutz kritischer Informations-Infrastrukturen in Österreich. Eine Kernaufgabe ist die rechtzeitige Vorsorge in Kooperation mit öffentlichen Stellen sowie großen Unternehmen und Institutionen. Eine wichtige Aufgabe ist es, die richtigen Informationen rechtzeitig zur Verfügung zu stellen.

Nach zwei Jahren des Betriebes lässt sich ein Resümee ziehen über die Aktivitäten, und wir wollen erstmals einen Jahresbericht zur Lage der IT-Sicherheit in Österreich vorlegen. Er beschreibt aktuelle Entwicklungen und Szenarien im Bereich der Internetsicherheit, Herausforderungen und Gegenstrategien, sowie die Leistungen des CERT in diesem Zusammenhang – national und in Abstimmung mit seinem europäischen und globalen Netzwerk. Experten geben Einblick in die Trends im Cybercrime, und auch Hilfe zur Selbsthilfe wird geboten.

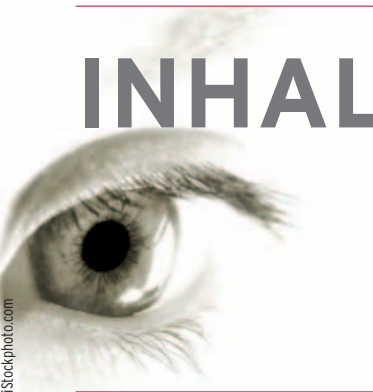
Dieser Bericht ist eine Premiere, Fortsetzungen sollen folgen. Im Interesse einer kontinuierlichen Weiterentwicklung und Verbesserung in den kommenden Jahren geben Sie uns bitte Feedback zum Bericht auf den Websites www.cert.at und www.govcert.gv.at.

Robert Schischka,
Leiter von CERT.at

© HBF

Roland Ledinger,
Leiter des Bereiches
IKT-Strategie des
Bundes im
Bundeskanzleramt

# INHALT




Vorwort Josef Ostermayer ..... 2
Vorwort Robert Schischka und Roland Ledinger ..... 3
Der Faktor Internet in Österreich ..... 4
Was bedeutet CERT? ..... 8
Strategische Infrastrukturen – Ein Kommentar von Walter J. Unger ..... 14
Cybercrime: Was kommt und was bleibt ..... 16
Hilfe zur Selbsthilfe ..... 20
Das CERT-Alphabet ..... 22


**IMPRESSUM:** Medieninhaber und Verleger: Computer Emergency Response Team Austria, Karlsplatz 1/3, 1010 Wien. Diese Publikation wurde in Kooperation mit dem Bundeskanzleramt erstellt. **Projektleitung:** Mag. Robert Schischka, CERT und Ing. Roland Ledinger, BKA. **Konzeption und Redaktion:** Pleon Publico Public Relations & Lobbying (David Mock, Ursula Eysin, Andrea Wilhelm) **Grafik:** creativedirector.cc lachmair gmbh. **Verlags- und Herstellungsort:** Wien. Juli 2010

# FAKTOR INTERNET IN ÖSTERREICH

**Das Internet: Motor für die Gesellschaft und Nervengeflecht für die Wirtschaft. Je größer die Bedeutung des Internets, desto wichtiger der Schutz der Informations- und Kommunikationstechnologie-Systeme (IKT).**

Die Anzahl der österreichischen Haushalte, die an das Internet angeschlossen sind, hat sich zwischen 2002 und 2009 von 33,5% auf 69,8% mehr als verdoppelt. Bei der Internetanbindung und der IKT-Nutzung pro Haushalt, pro Unternehmen sowie bei der Regierung liegt Österreich überall über dem EU-Durchschnitt. Laut OECD Information Technology Outlook 2008 hat die Zahl der Branchen und Berufe, in denen IKT eingesetzt werden, innerhalb der EU ganz besonders in den skandinavischen Ländern, in Irland und in Österreich zugenommen. Die Gesamtausgaben für IKT sind in Österreich von 2003 bis 2008 um mehr als 50% gewachsen, im OECD-Durchschnitt nur um knapp 42%.

Besonders im Bereich E-Government ist Österreich Vorreiter: Der Einfluss der Informationstechnologie auf die öffentliche Verwaltung hat mit der E-Government-Offensive seit 2001 enorm zugenommen. Österreich konnte im europäischen E-Government Benchmarking 2006 von Platz 13 aus den Spitzenplatz erobern und bis heute halten.

Die heimische Wirtschaft hat das enorme Potential zur Produktivitätssteigerung durch die moderne Informations- und Kommunikationstechnologie frühzeitig erkannt und kann im globalen Wettbewerb durch permanente Technologieanpassung und -weiterentwicklung bestehen. Damit ist die österreichische Wirtschaft mittlerweile aber auch stark vom Funktionieren der Informations- und Kommunikationsflüsse abhängig. Die zunehmende Abhängigkeit der Informationsgesellschaft von ihren Informations- und Kommunikationssystemen einerseits und die Verwundbarkeit dieser Systeme andererseits schaffen Angriffspunkte. Diese können gezielt genutzt werden, um die Informationsgesellschaft oder Teile davon zu schwächen oder sogar zu zerstören.

Ein massiver Angriff auf das IKT-System eines Staates oder einer Gesellschaft hat damit unter Umständen ähnliche Wirkungen wie ein massiver Angriff auf die industrielle Basis. Cyberattacken durch Würmer, Viren und andere virtuelle Schädlinge können erheblichen wirtschaftlichen Schaden anrichten.

© michele piacquadio - iStockphoto.com




## Schädlingsbefall auf österreichischen PCs

Derzeit gibt es kaum eine präzise, einheitliche und fundierte Sicht auf die „Gesamtdurchseuchungsrate" des Internets bzw. von Windows PCs. Die umfassendste Erhebung zu dieser Fragestellung ist der Microsoft Security Incident Report (SIR), der vom weltweit tätigen Software-Konzern zwei Mal jährlich herausgegeben wird. Microsoft stellt das sogenannte Malicious Software Removal Tool (MSRT) gratis zur Verfügung, welches PCs auf die gängigste Schadsoftware wie Viren, Würmer und Trojaner ("Malware") hin untersucht. Das macht auch einen internationalen Vergleich des Schädlingsbefalls österreichischer PCs möglich.
Wie im aktuellen Security Report von Microsoft erkennbar, ist Österreich im Bezug auf Botnetze und Malware generell sehr "sauber". Das hat vermutlich mehrere Gründe, so etwa:

- Automatische Updates sind oft aktiviert, was zum Basisschutz des PCs beiträgt. Das korreliert wiederum mit dem vergleichsweise niedrigen Anteil an unlizensierten Versionen von Windows.

- Die österreichischen Internet Service Provider (ISPs) reagieren auf Beschwerden bezüglich verseuchter PCs besser und konsequenter als die vieler anderer Länder.

Im Fall des Wurms Conficker hat selbst das regelmäßige Update lizensierter Versionen wenig geholfen, da der Wurm über vielfältige Infektionsmethoden verfügt und kein Virenschutz hundertprozentig Sicherheit bieten kann.

Aktuell sind in Österreich rund 12.000 PCs mit Conficker.A oder .B und rund 300 mit Conficker.C infiziert. Über den gesamten Infektionsverlauf hinweg befand sich Österreich im internationalen Mittelfeld.

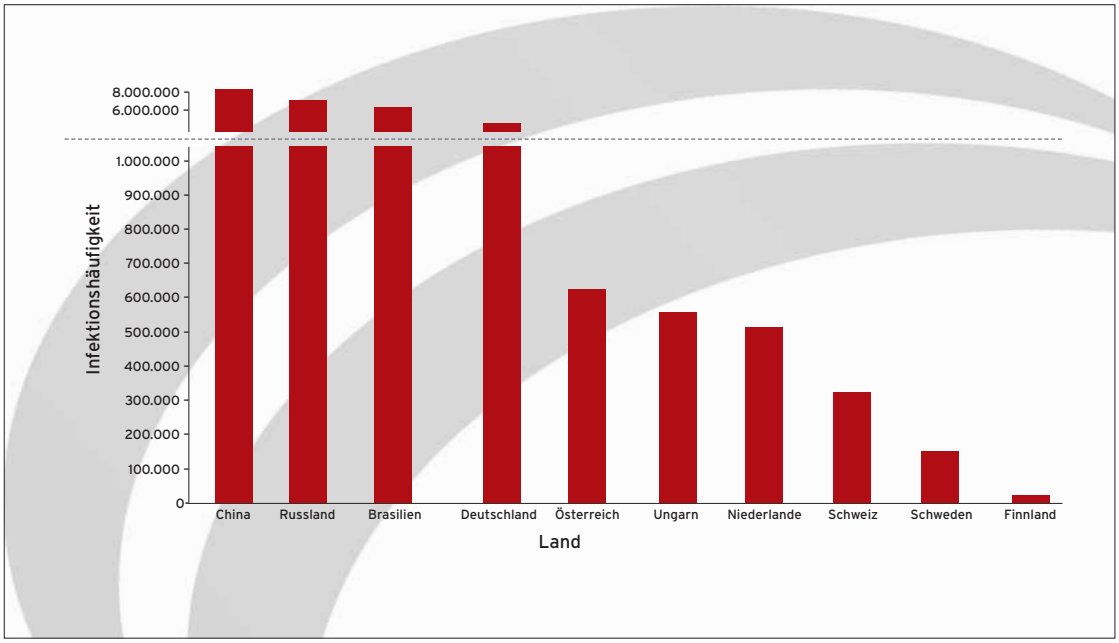



**Abbildung 1:** Infektionshäufigkeit je Land durch Conficker (Internet-Wurm): Vor allem China, Brasilien und Russland waren stark betroffen. Österreich dagegen hatte eine relativ niedrige Infektionsrate.



## Österreichische Domains zählen zu den sichersten der Welt

Wie die 2009 vom Sicherheits-Dienstleister McAfee veröffentlichte Studie „Mapping the Mal Web – The World's Riskiest Domains" zeigt, gehören .at-Domains zu den sichersten der Welt.

Gemeinsam mit der Schweiz, Irland, Luxemburg oder Japan befindet sich Österreich damit in punkto Domainsicherheit im absoluten Spitzenfeld.

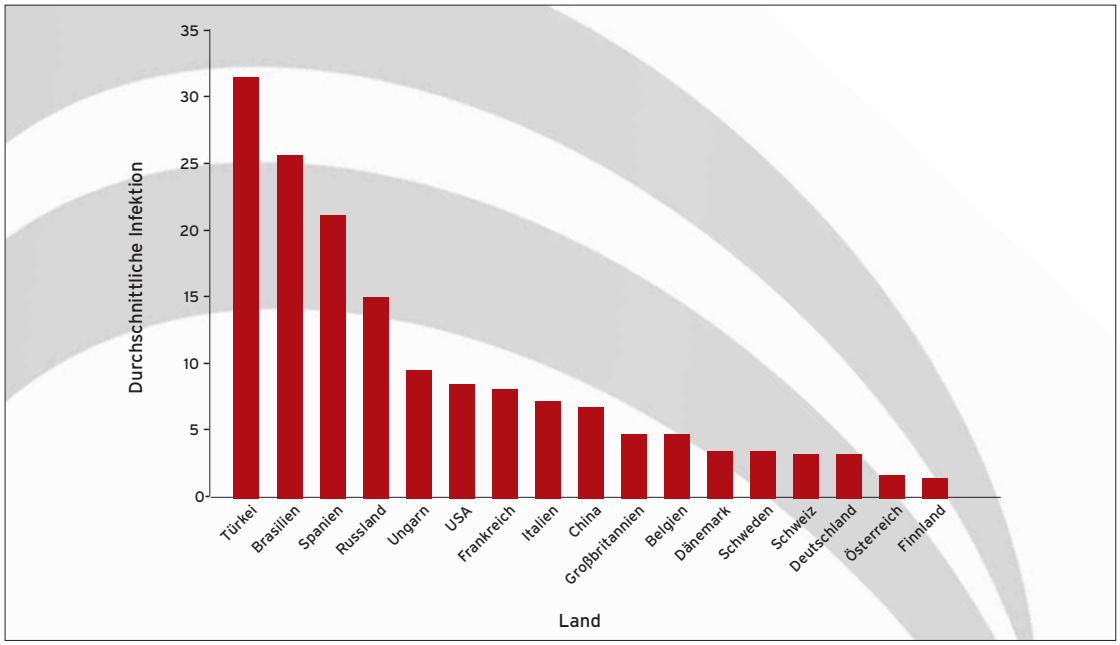
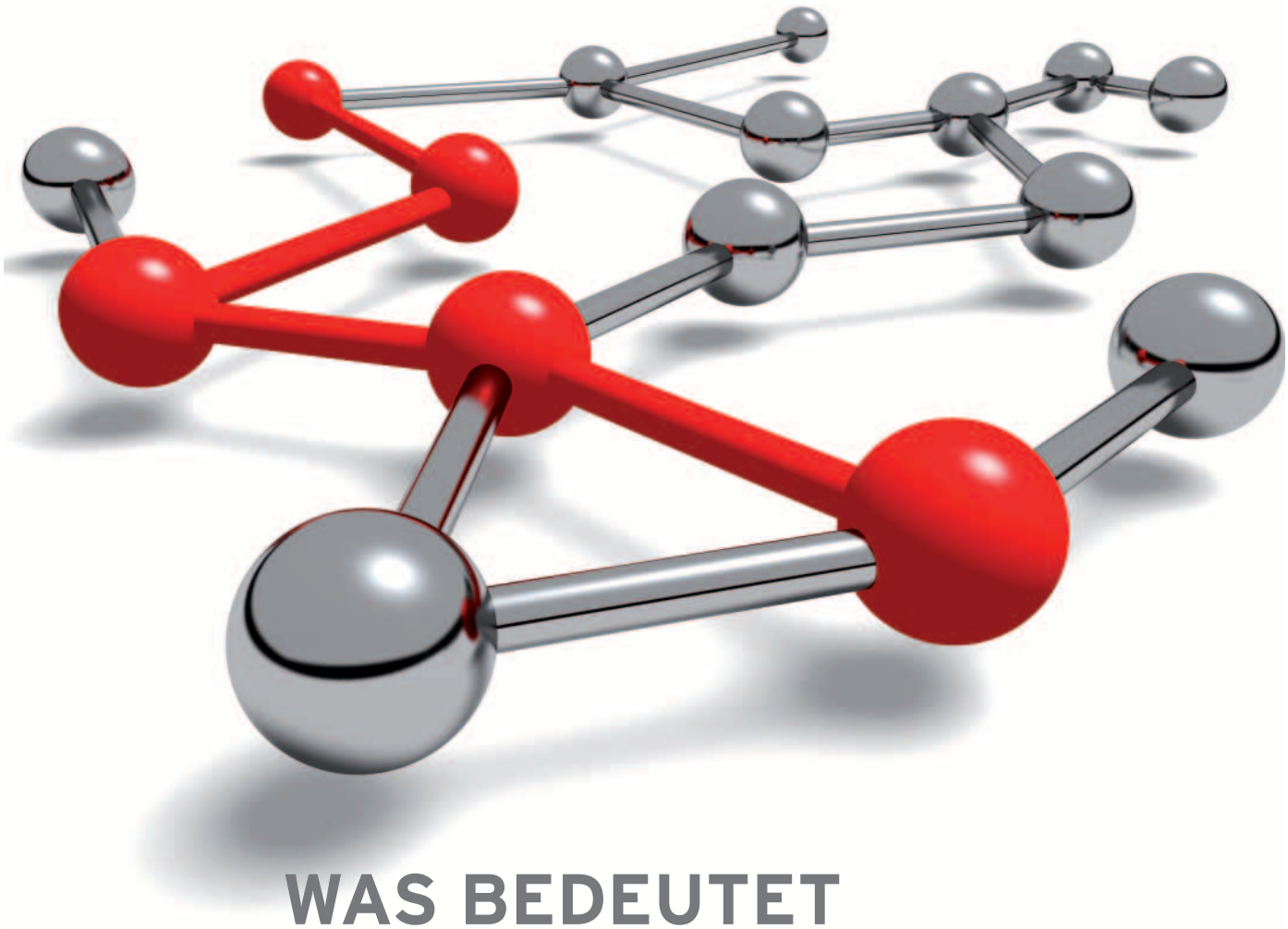



**Abbildung 2:** Zahl der entfernten Schadsoftware pro tausend Ausführungen des Malicious Software Removal Tools. Österreich hat sich im Vergleich zum Jahr 2008 verbessert und liegt mit 2,1 infizierten PCs pro tausend Ausführungen im absoluten Sicherheits-Spitzenfeld – nur Finnland weist bessere Werte auf.





# WAS BEDEUTET CERT ?

**Computer Emergency Response Team – im Interesse der Sicherheit von Informationstechnologien. In Österreich und weltweit.**

1988 legte der erste Internet-Wurm weltweit eine beträchtliche Anzahl von IT-Systemen lahm. Angesichts der offensichtlichen Notwendigkeit eines raschen und effizienten Informationsaustausches zwischen Systembetreibern in solchen Krisenfällen wurde kurz darauf das erste Computer Emergency Response Team an der Carnegie Mellon University in Pittsburgh (USA) gegründet.

1992 entstand die erste europäische Einrichtung dieser Art in den Niederlanden. Heute zählt die European Network and Information Security Agency (ENISA) in ihrem Inventory of CERT Activities in Europe (www.enisa.europa.eu/act/cert/background) weit über 100 Mitgliedsorganisationen auf.

Im Folgenden wird durchgehend der Ausdruck CERT verwendet, obwohl häufig auch von CSIRT (Computer Security Incident Response Team) gesprochen wird. Weitere gebräuchliche Abkürzungen sind SERT, CIRT, IRT oder z.B. auch WARP (Warning, Advice and Reporting Point).

## CERT.at und GovCERT in Österreich

CERT.at und GovCERT.at wurden 2007 als gemeinsame Initiative von Bundeskanzleramt und der Internet Foundation Austria (IPA) gegründet und nahmen im März 2008 ihre operative Arbeit auf. Seither sind sie erste Anlaufstelle für Fragen zur Sicherheit im österreichischen Teil des Internets, wobei sie sich an kleine und mittlere Unternehmen sowie an den öffentlichen Sektor richten, an Banken, Institutionen des Gesundheitswesens, große Infrastrukturbetreiber (Telekom, Energie, öffentlicher Verkehr) – also an alle, die „kritische Infrastruktur“ zur Verfügung stellen.

Die konkreten CERT-Leistungen sind vielfältig, im Zentrum steht aber immer die aktuelle und bewertete Information zu akuten Sicherheitsbedrohungen im Internet. Entweder auf Basis eigener Recherchen oder nach Verständigung durch betroffene Stellen oder ausländische CERTs werden die Experten aktiv und leiten die notwendigen Schritte ein. Diese können zum Beispiel die Distribution bestimmter Tools und Programme sein, um aktiv gegen Sicherheitsbedrohungen vorzugehen. Sie umfassen aber auch Analysen und detaillierte Warnungen vor bestimmten Gefahren und die Recherche zu möglichen Bedrohungen für die Internet-Sicherheit in der Zukunft.

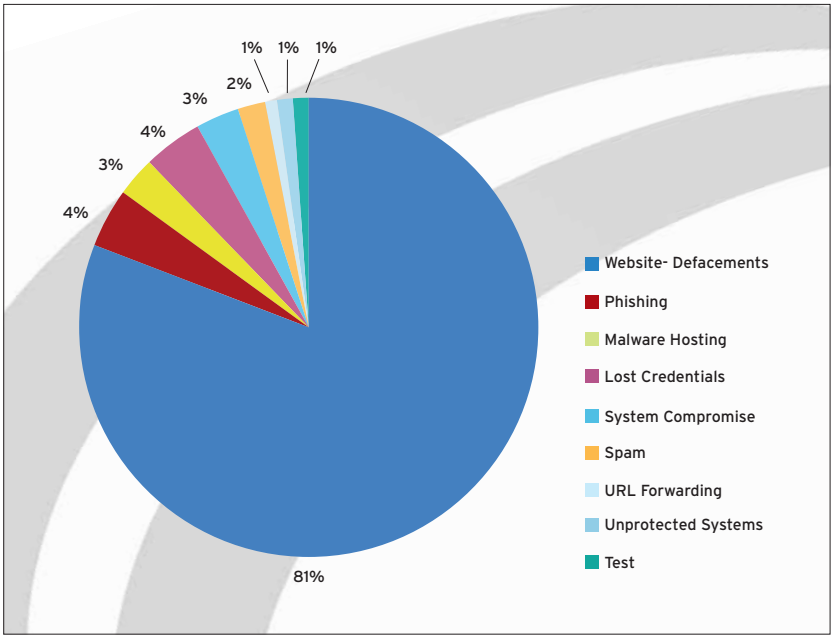



Abbildung 3: Incidents nach Gruppen

## Herausforderungen: Information für alle

Eine besondere Herausforderung dabei: Das Informationsniveau der Zielgruppen ist sehr unterschiedlich. Große Unternehmen mit eigener IT-Abteilung verlangen nach einer anderen Art der Information als zum Beispiel kleine und mittlere Unternehmen (KMU) oder Privatpersonen.

CERT.at und GovCERT.at umfassen derzeit ein Team von sieben erfahrenen IT-Experten. Sie stimmen sich dabei eng mit den Experten verschiedener Institutionen ab. Zum Zweck der raschen und kurzfristigen Unterstützung bei der Schadensbehebung im Notfall, wenn eine betroffene Organisation nicht über genügend eigene Fachleute zur Bewältigung der unmittelbar notwendigen Reparaturmaßnahmen verfügt, hat das GovCERT darüber hinaus einen Expertenpool der öffentlichen Verwaltung gegründet. Dieser bildet eine Art freiwillige Feuerwehr, die bei Bedarf zu Hilfe gerufen werden kann, wenn es um die rasche Wiederherstellung des Normalbetriebes der IKT geht. Da sich dieser Pool nicht allein aus Dienststellen in Wien rekrutiert, sollte damit Sicherheitsvorfällen im gesamten Bundesgebiet mit einer vertretbaren Reaktionszeit und einem angemessenen wirtschaftlichen Aufwand begegnet werden können.

Als einer der größten Meilensteine im ersten Jahr gilt die rasche und erfolgreiche Bekämpfung des Conficker Wurms – hier konnte sehr rasch die Gefahr erkannt und Hilfe organisiert werden. Details dazu gibt es ab Seite 16 dieses Berichts.

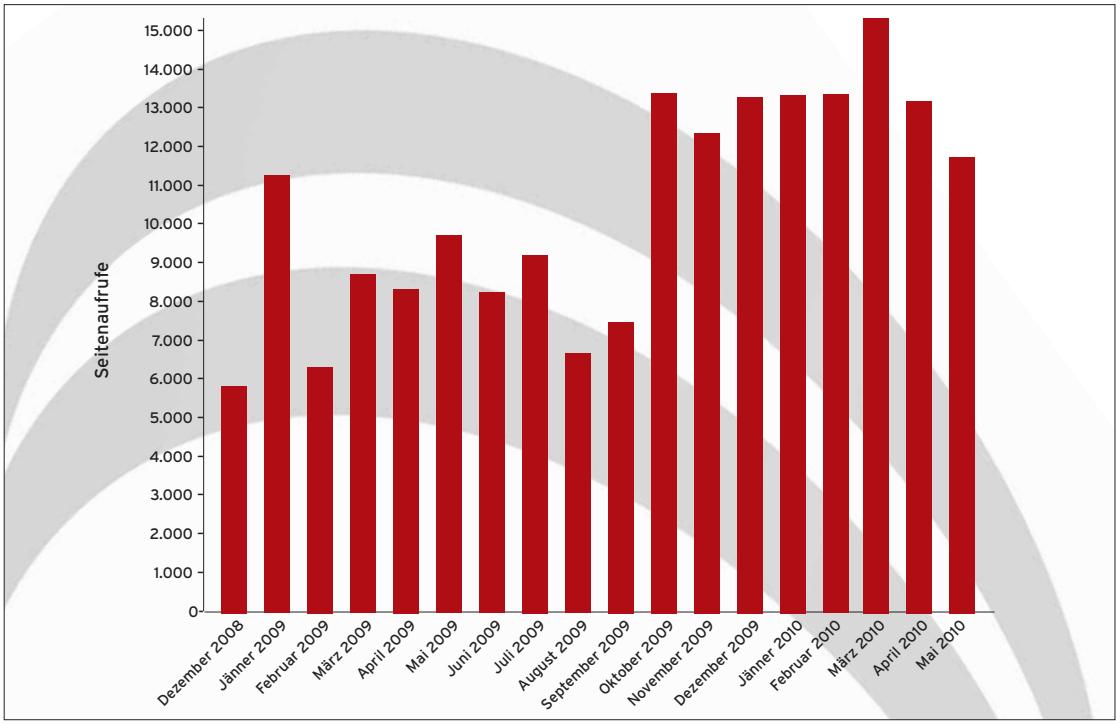



Abbildung 4: Zugriffe auf die CERT.at-Homepage seit September 2008

Die Sicherheitswarnungen können auf www.cert.at abonniert werden, Meldungen und Anfragen nimmt CERT.at auch per Mail unter reports@cert.at oder von Montag bis Freitag zwischen 8 und 18 Uhr telefonisch unter 01 / 505 64 16 78 entgegen. Der Kundenkreis öffentliche Verwaltung und kritische Infrastruktur kann sich per Mail auch an post@govcert.gv.at wenden.
Die Meldungen an CERT.at teilen sich in Informationsmeldungen und tatsächliche Vorfälle, denen nachgegangen werden muss – sogenannte „Incidents“. Diese werden bearbeitet, bis das Problem gelöst ist. Dabei gibt es oft mehrere Aktionen ("Investigations") pro Vorfall. Seit Bestehen wurden über 2.300 Incidents bearbeitet, daraus folgten rund 3.700 Investigations mit den jeweils betroffenen Unternehmen und Institutionen, um die Probleme zu lösen.

## CERT, Europa und die Welt – Die internationale Vernetzung

Sicherheitsvorfälle im Internet beschränken sich nur sehr selten auf ein einzelnes Land: Sicherheitslücken in Standardkomponenten wie dem Betriebssystem oder dem Browser treten unabhängig vom Einsatzort der Software auf. Werden diese Schwachstellen über das Internet ausgenutzt, so sitzt der Täter oft im Ausland.

Es ist daher für nationale CERTs essentiell, mit ihren Schwesterorganisationen im Ausland zusammenzuarbeiten. Durch ihre Mitgliedschaft bei internationalen Foren können CERT.at und GovCERT.at auf eine Reihe starker Kooperationspartner weltweit zurückgreifen.

**Die Kooperation mit ausländischen CERTs umfasst folgende Schwerpunkte:**

- Die verschiedenen CERTs tauschen Informationen über aktuelle Warnungen und neu bekannt gewordene Schwachstellen bei Standardsoftware untereinander aus. Hier spielen die Sicherheitsteams der Hersteller eine zentrale Rolle. Ob der Masse an Informationen in öffentlichen Quellen (Mailinglisten, Webseiten, Blogs, ...) sind aber andere CERTs als Filter und Bewerter von Ankündigungen sehr hilfreich.

- Konkrete Vorfälle (Einbrüche in Rechner, Phishing, Spam, etc.) sind nur selten auf ein Land beschränkt: auch hier informieren die nationalen CERTs einander über Vorfälle im jeweiligen Verantwortungsbereich.

- Da jedes CERT an ähnlichen Problemstellungen arbeitet, lassen sich durch Kooperationen Synergieeffekte nutzen: Das umfasst unter anderem spezialisierte Software, die für den Betrieb eines CERT benötigt wird, Analyseergebnisse von Schadsoftware oder auch einfach nur gesammelte Kontaktinformationen.

- Bei Treffen und Konferenzen kommt es zwischen den internationalen CERT-Experten zu einem regen Informationsaustausch. Neben den Fachvorträgen, zu denen Österreich immer wieder wichtige Beiträge leistet, wird auch die intensive Vernetzung gesucht.

Um die internationale Kooperation zu erleichtern und zu institutionalisieren, haben sich in den letzten Jahren diverse Verbände und Foren etabliert, über die CERTs und andere IT-Sicherheitsteams kommunizieren.
Nicht alle diese Foren sind etablierte Organisationen, ein beträchtlicher Teil der Kommunikation läuft auch über Mailinglisten und Foren, die aus Initiativen einzelner Personen entstanden sind. Ein gutes Beispiel für eine ad-hoc Zusammenarbeit ist die Conficker Working Group (www.confickerworkinggroup.org), in der auch Österreich aktiv mitarbeitet.

**Hier ein paar Details zu den wichtigsten offiziellen Foren:**

- FIRST (Forum of Incident Response and Security Teams, www.first.org) ist der weltweite Dachverband der CERT-Community und zählt derzeit über 200 Mitglieder in 48 Ländern. Die jährliche FIRST-Konferenz ist der wichtigste internationale Branchen-Treff für CERT-Experten – CERT.at ist seit 2008 FIRST-Mitglied und seit kurzem mit Robert Schischka auch im Steering Commitee vertreten.

- TF-CSIRT (Taskforce Computer Security Incident Response Teams, www.terena.org/activities/tf-csirt) ist unter dem Dach des Verbandes der Wissenschaftsnetze Europas gewachsen. Der Fokus liegt hier eindeutig auf Europa. TF-CSIRT trifft sich dreimal pro Jahr zu Fachvorträgen mit dem Ziel, die Zusammenarbeit untereinander zu stärken. Auch CERT.at ist Mitglied bei diesem Forum.

- Aus diesen Bemühungen ist der TI (Trusted Introducer www.trusted-introducer.org), eine Datenbank aller akkreditierten CERTs in Europa, hervorgegangen.

- Das US-CERT (aus dem ursprünglichen CERT der Carnegie-Mellon Universität gewachsen) organisiert jährliche Treffen von nationalen CERTs, auch dabei ist Österreich vertreten.

- CERT.at und GovCERT.at nehmen an den Treffen des deutschen CERT-Verbundes (www.cert-verbund.de) teil und kooperieren eng mit dem deutschen Bundesamt für Sicherheit in der Informationstechnik und mit dem Schweizer Informatikstrategieorgan Bund.

- Ein Mitgliedsantrag von GovCERT.at bei der European Government CERTs Group (www.egc-group.org) wird gerade geprüft.

Die European Network and Information Society Agency der EU (www.enisa.europa.eu) führt CERT.at und GovCERT.at folglich als erste Kontaktadressen für Fragen der IT-Security in Österreich an. CERT.at hat mit zahlreichen anderen CERTs regelmäßigen Kontakt und Datenaustausch. Zwei sehr konkrete Beispiele für diese internationale Zusammenarbeit sind die Kooperationen mit AusCERT und CERT.br, die in Folge etwas detaillierter dargestellt werden.

# Der CERT-Beirat

Um CERT.at in seiner strategischen Ausrichtung zu unterstützen, wurde der CERT-Beirat eingerichtet. Als beratendes Organ bringt er aktiv seine Themenvorschläge und Sichtweisen ein. Die Mitglieder des Beirats setzen sich gemäß eines repräsentativen Querschnitts der Internet-Community in Österreich zusammen und werden für jeweils drei Jahre gewählt. Außerdem fungieren sie als Botschafter von CERT.at und GovCERT und unterstützen damit die Vernetzung des Themas Internetsicherheit in Gesellschaft und Politik.

Momentan besteht der CERT-Beirat aus folgenden Personen:

- Ing. Roland Ledinger (BKA)
- Mag. Günther Simonitsch (BMI)
- Ing. Franz Hoheiser-Pförtner, MSc (Krankenanstaltenverbund)
- Wilfried Wöber (Universität Wien)
- Prof. Dr. Nikolaus Forgó (Universität Wien)
- Thomas Mandl (Selbständiger Experte)

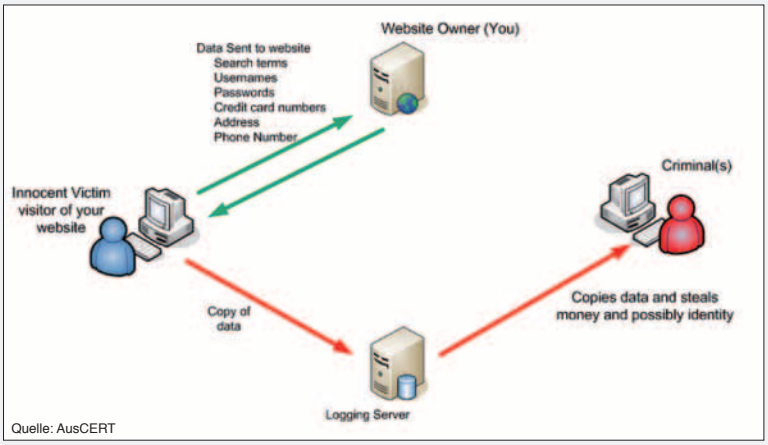
CERT.at wurde auf Initative des BKA und der Internet Foundation Austria (IPA) gegründet. Die IPA ist eine gemeinnützige österreichische Stiftung, deren Stiftungszweck es ist, das Internet in Österreich zu fördern. Weiters übernimmt sie mittels nic.at die Verantwortung der Internet-Domainregistrierung und -verwaltung für Österreich (.at, .co.at und .or.at). nic.at zeichnet auch für die operative Abwicklung von CERT.at verantwortlich.

# Verlorene Zugangsdaten: Australien sammelt für die Welt

Bei dieser Kooperation beliefert das australische CERT (AusCERT) das österreichische CERT.at mit gestohlenen Zugangsdaten (Username, Passwort). CERT.at wiederum macht die Benutzer bzw. Serviceanbieter darauf aufmerksam, dass sie ihre Zugangsdaten aufgrund von Malware-Infektionen verloren haben.

## Wie funktioniert das?

AusCERT beobachtet einige Botnetze und vor allem Command und Control (C&C) Server dieser Botnetze. Manche dieser C&C Server werden dazu verwendet, die ausspionierten Daten von allen infizierten PCs zu sammeln (sogenannte “Drop Boxes”, “Logging Server”). Welche Daten die Malware sammelt, kann variieren: die Palette reicht von im Browser gespeicherten Zugangsdaten, Konfigurationseinstellungen von Mailprogrammen, Formulareingaben bis zu Mitschnitten von Tastatureingaben. Kriminelle können sich auf diesem Weg Zugriff auf viele Internetdienste (Email, Social Media, Online-Banking, …) verschaffen und diesen entsprechend missbrauchen.



Quelle: AusCERT

Findet AusCERT diese gestohlenen Zugangsdaten auf Drop Boxes, dann werden diese nach dem Land der betroffenen Dienste geordnet und an die entsprechenden nationalen CERTs weitergegeben. CERT.at verteilt diese Informationen in Österreich weiter. Der Betreiber der Webseite kann dann entsprechend reagieren, indem er den Account als kompromittiert behandelt und den betroffenen Benutzer informiert und warnt. Meist ist das Problem für den Benutzer erledigt, wenn der Benutzer seine Zugangsdaten geändert hat und seinen PC gründlich auf Viren und Malware untersucht hat.

CERT.at kontaktiert zwar auch die Betreiber von Webseiten, diese müssen aber nicht unbedingt selbst eine Schwachstelle haben. Häufig liegt das Problem auf Seiten des Benutzer-PCs, wo mittels Schadsoftware Zugangsdaten abgegriffen wurden. Gerade im Kontext von Online-Banking zeigt dies wiederholt die Notwendigkeit zusätzlicher Maßnahmen wie etwa eines sicheren Zweitkanals wie beispielsweise SMS.

Auf diese Weise konnte CERT.at gemeinsam mit AusCERT im Jahr 2009 schon mehrere Tausend Internetbenutzer informieren, die auf 5.633 verschiedenen Webservern in Österreich ihre Zugangsdaten verloren haben. Dabei waren 1.033 .at-Domains involviert. Die Bandbreite der betroffenen Websiten ist groß und reicht von Webmailern über Partnerbörsen bis hin zu Finanzdienstleistern.



# Mail Spamtraps

CERT.at betreibt gemeinsam mit dem brasilianischen nationalen CERT (CERT.br) einen Mail Spamtrap Server. Unter einem Spamtrap Server versteht man einen Server, der vorgibt, ein offener Relay zu sein. D.h. der Server gibt vor, jede Mail, die aus dem Internet an ihn geschickt wird, an beliebige Ziel-Adressaten weiterzuleiten.

**CIDR Blocks**

**Top 15 CIDR Blocks sorted by emails**

| # | CIDR block | ASN | CC | emails (%) | | recipients (%) | | connections | proto |
|---|---|---|---|---|---|---|---|---|---|
| 1 | [redacted] | [redacted] | TW | 354 | 11.38 | 10,624 | 13.63 | 131 | SMTP |
| 2 | [redacted] | [redacted] | US | 273 | 8.77 | 2,730 | 3.50 | 273 | SMTP |
| 3 | [redacted] | [redacted] | TW | 242 | 7.78 | 4,063 | 5.21 | 154 | HTTP, S5 |
| 4 | [redacted] | [redacted] | TW | 222 | 7.13 | 6,641 | 8.52 | 86 | HTTP, SMTP, S5 |
| 5 | [redacted] | [redacted] | HK | 221 | 7.10 | 3,724 | 4.78 | 110 | HTTP, S4, S5 |
| 6 | [redacted] | [redacted] | HK | 172 | 5.53 | 2,846 | 3.65 | 88 | HTTP, S4, S5 |
| 7 | [redacted] | [redacted] | HK | 168 | 5.40 | 2,690 | 3.45 | 85 | HTTP, S4, S5 |
| 8 | [redacted] | [redacted] | US | 142 | 4.56 | 5,791 | 7.43 | 68 | HTTP, S4, S5 |
| 9 | [redacted] | [redacted] | US | 128 | 4.11 | 5,209 | 6.69 | 50 | HTTP, S4, S5 |
| 10 | [redacted] | [redacted] | FR | 125 | 4.02 | 1,250 | 1.60 | 125 | SMTP |
| 11 | [redacted] | [redacted] | US | 70 | 2.25 | 2,969 | 3.81 | 35 | HTTP, S4, S5 |
| 12 | [redacted] | [redacted] | TW | 60 | 1.93 | 1,638 | 2.10 | 27 | SMTP |
| 13 | [redacted] | [redacted] | US | 51 | 1.64 | 1,738 | 2.23 | 16 | HTTP, S4 |
| 14 | [redacted] | [redacted] | US | 48 | 1.54 | 1,681 | 2.16 | 21 | HTTP, S4, S5 |
| 15 | [redacted] | [redacted] | US | 46 | 1.48 | 1,613 | 2.07 | 23 | HTTP, S4 |
| 16 | others (160) | | | 790 | 25.39 | 22,713 | 29.15 | 289 | 0, HTTP, SMTP, S4, S5 |
| **Total** | | | | **3,112** | **100.00** | **77,920** | **100.00** | **1,581** | |

**Top 15 CIDR Blocks sorted by recipients**

| # | CIDR block | ASN | CC | recipients (%) | | emails (%) | | connections | proto |
|---|---|---|---|---|---|---|---|---|---|
| 1 | [redacted] | [redacted] | TW | 10,624 | 13.63 | 354 | 11.38 | 131 | SMTP |
| 2 | [redacted] | [redacted] | TW | 6,641 | 8.52 | 222 | 7.13 | 86 | HTTP, SMTP, S5 |
| 3 | [redacted] | [redacted] | US | 5,791 | 7.43 | 142 | 4.56 | 68 | HTTP, S4, S5 |
| 4 | [redacted] | [redacted] | US | 5,209 | 6.69 | 128 | 4.11 | 50 | HTTP, S4, S5 |
| 5 | [redacted] | [redacted] | TW | 4,063 | 5.21 | 242 | 7.78 | 154 | HTTP, S5 |
| 6 | [redacted] | [redacted] | HK | 3,724 | 4.78 | 221 | 7.10 | 110 | HTTP, S4, S5 |
| 7 | [redacted] | [redacted] | US | 2,969 | 3.81 | 70 | 2.25 | 35 | HTTP, S4, S5 |
| 8 | [redacted] | [redacted] | HK | 2,846 | 3.65 | 172 | 5.53 | 88 | HTTP, S4, S5 |
| 9 | [redacted] | [redacted] | US | 2,730 | 3.50 | 273 | 8.77 | 273 | SMTP |
| 10 | [redacted] | [redacted] | HK | 2,690 | 3.45 | 168 | 5.40 | 85 | HTTP, S4, S5 |
| 11 | [redacted] | [redacted] | US | 1,849 | 2.37 | 42 | 1.35 | 17 | HTTP, S4 |
| 12 | [redacted] | [redacted] | US | 1,738 | 2.23 | 51 | 1.64 | 16 | HTTP, S4 |
| 13 | [redacted] | [redacted] | US | 1,682 | 2.16 | 37 | 1.19 | 14 | HTTP, S4, S5 |
| 14 | [redacted] | [redacted] | US | 1,681 | 2.16 | 48 | 1.54 | 21 | HTTP, S4, S5 |
| 15 | [redacted] | [redacted] | US | 1,662 | 2.13 | 38 | 1.22 | 19 | HTTP, S4 |
| 16 | others (160) | | | 22,021 | 28.26 | 904 | 29.05 | 414 | HTTP, SMTP, S4, S5 |
| **Total** | | | | **77,920** | **100.00** | **3,112** | **100.00** | **1,581** | |

Durch die Kooperation mit CERT.br gelangt CERT.at an eine grössere Menge an Spam-Statistiken und Malware, die per Mail verschickt wird.
CERT.at erhält somit einen Überblick, welche IP Adressen und Netzwerkblöcke versuchen, offene Mail-Relays zu finden und zu missbrauchen.

# STRATEGISCHE INFRASTRUKTUREN - DURCH CYBER WAR UND CYBER TERRORISMUS BEDROHT

Das Funktionieren von Infrastrukturen mit strategischer Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen ist kritisch für den Staat als Ganzes. Störungen oder Zerstörungen dieser Infrastrukturen haben schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit, das wirtschaftliche und soziale Wohl der Bevölkerung oder die effektive Funktionsweise von staatlichen Einrichtungen. Im europäischen Programm für den Schutz kritischer Infrastrukturen werden 11 Sektoren angeführt: Energie, Nuklearindustrie, IKT, Wasser, Lebensmittel, Gesundheit, Finanzen, Transport, Chemische Industrie, Raumfahrt und Forschungseinrichtungen.
Die zentralen Kommunikationsknoten und Steuerungssysteme dieser einer modernen Gesellschaft zur Verfügung stehenden Infrastrukturen basieren auf Informations- und Kommunikationstechnologie oder sind für die IKT von erheblicher Bedeutung und nur in bestimmten Objekten funktionsfähig. Das geht einher mit einer stark steigenden Abhängigkeit von Staat, Wirtschaft und Gesellschaft vom ordnungsgemäßen, einwandfreien und sicheren Funktionieren der IKT.

Die groß angelegten Cyber-Angriffe gegen staatliche Infrastrukturen Estlands im Frühling 2007 sowie im Krieg gegen Georgien im August 2008 zeigen den Bedeutungswandel und den akuten staatlichen Handlungsbedarf zum Schutz der nationalen strategischen Infrastruktur auf. Die zunehmende Abhängigkeit der Informationsgesellschaft von ihren Informations- und Kommunikationssystemen einerseits und die Verwundbarkeit dieser Systeme andererseits schaffen Angriffspunkte, die gezielt genutzt werden könnten, um eine Informationsgesellschaft oder Teile davon zu schwächen oder sogar zu zerstören.

Es ist daher notwendig, den Blick für die Bedeutung und Verwundbarkeit der strategischen Infrastruktur zu schärfen. Aus dem erkennbaren Bedrohungspotenzial sind Konsequenzen für das staatliche Handeln abzuleiten.

## Bedrohungspotenzial Cyber War (CW) und Cyber Terrorismus (CT)

Unter Cyber War (CW)/ Cyber Terrorismus (CT) wird „die absichtliche Beeinträchtigung der gegnerischen Informationen, Informationssysteme und durch Information gestützten Prozesse zur Erreichung der Informationsüberlegenheit und letztlich zur Durchsetzung eigener politisch- strategischer Ziele“ verstanden.
Mutmaßliche Angriffsziele für CW/CT–Attacken stellen die Grundwerte – Verfügbarkeit, Vertraulichkeit, Integrität – der strategischen, auf IKT basierenden Infrastrukturen eines Staates dar. Ein Angriff kann aufgrund der weltweiten Vernetzung von jedem Punkt der Erde ausgehen. Die Nachvollziehbarkeit und Identifikation als eine von außen kommende Bedrohung wird dadurch erheblich erschwert. Die geringen Kosten für die Durchführung eines Angriffes erweitern den potenziellen Täterkreis. Nicht nur Staaten, sondern auch Terrorgruppen und sogar Einzeltäter kommen als Angreifer in Frage. Angriffe auf die IKT werden daher entweder als ein „bewaffneter Angriff“ im Sinne des Artikels 51 der UN-Charta oder als ein politischer oder allgemein „krimineller Akt“ zu qualifizieren sein. Politische, ideologische, religiöse, ethnische aber auch ökonomische, anarchistische oder persönliche Motivationen sind möglich. Insgesamt ist ein breites Spektrum von Angreifern, Tätern und deren Motivation vorstellbar.

Das konkrete Ausmaß der allfällig verursachbaren Schäden kann nur nach einer Detailanalyse eingeschätzt werden, da insbesondere der Vernetzungsgrad und die dadurch entstandenen Abhängigkeiten zwischen den strategischen IKT–Ressourcen nicht ausreichend bekannt sind.

CW/CT stellte schon in der Gegenwart ein erhebliches subkonventionelles Risiko für die nationale Sicherheit dar. Potenziell betroffene Behörden und Wirtschaftsunternehmen haben für den Eigenschutz vorzusorgen. Kriminelle Akte sind durch die Strafverfolgungsbehörden (Justiz und Sicherheitspolizei) zu bekämpfen. Art und Umfang von kriminellen Akten könnten diese zuständigen staatlichen Sicherheitseinrichtungen überfordern und eine Inanspruchnahme spezieller Fähigkeiten und Kräfte erfordern. Die Abwehr von Angriffen auf die nationale Sicherheit mit CW-Mitteln könnte eine neue Aufgabe der militärischen Landesverteidigung sein.

## Strategie IKT- Sicherheit in Österreich

Österreichs Transformation ins Informationszeitalter ist weit fortgeschritten. Österreich ist in erheblichem Ausmaß vom Funktionieren seiner kritischen Informationsinfrastrukturen abhängig. Während die Durchdringung mit IKT sehr rasch vorangeschritten ist, hinkt die Nachhaltigkeit durch einen Mangel an Absicherungsmaßnahmen hinterher.

Zwar hat Österreich mit der Verabschiedung der Sicherheits- und Verteidigungsdoktrin schon 2001 die Weiterentwicklung der Umfassenden Landesverteidigung zur Umfassenden Sicherheitsvorsorge begonnen. Mittlerweile sind als Antwort auf die neuen Herausforderungen unter dem Dach einer Gesamtstrategie 10 Teilstrategien entworfen. Die Teilstrategie IKT-Sicherheit sollte das Fundament eines strategischen IKT-Sicherheitskonzeptes sein.

Auf der Basis des 2004 begonnenen Europäischen Programmes für den Schutz kritischer Infrastrukturen wurde der Masterplan zur Erstellung des österreichischen Programms zum Schutz kritischer Infrastrukturen (APCIP = Austrian Program for Critical Infrastructure Protection) auf nationaler Ebene festgelegt. Der Masterplan beschreibt die Grundsätze des Programms, beinhaltet die Auflistung der vorrangig zu untersuchenden Sektoren, definiert Kriterien für die Einstufung kritischer Infrastrukturen, benennt die Risikofaktoren und die Akteure, listet die Maßnahmen zum Schutz kritischer Infrastrukturen auf und entwickelt einen Aktionsplan mit detaillierten Teilzielen.

Die Umsetzung der „Umfassenden Sicherheitsvorsorge“ und des APCIP wird nur durch Installierung der erforderlichen Strukturen möglich werden.

## Staatlicher Strukturbedarf

Von staatlicher Seite sind ausreichend Ressourcen für ein Instrument zur Analyse, Bewertung und Prognose von Entwicklungen der strategischen IKT einschließlich einer Risikobewertung, ein permanentes Lagezentrum zur Beobachtung und Bewertung der Bedrohungslage sowie für eine allfällige Frühwarnung, Alarmierung und Auslösung von Reaktionen und Notfallorganisationen (CERT/CSIRT) bereitzustellen.

Es bedarf einer zentralen Stelle in Österreich, die alle einschlägigen Informationen von Bundes- und Landesdienststellen sowie Privaten sammelt, analysiert, bewertet und in der Lage ist, die notwendigen Aufklärungs-, Vorbeugungs-, Abwehr- und Reaktionsmaßnahmen zu treffen bzw. verbindlich anzuordnen. Diese Stelle hat auch zweckmäßigerweise die Steuerung und Koordination der nationalen und internationalen Zusammenarbeit sicherzustellen. Die erforderlichen gesetzlichen Voraussetzungen wären zu schaffen.

**Mag. Walter J. Unger,**
Oberst des Generalstabsdienstes. Seit 1982 Kommandanten- und Leiterfunktionen in der Truppe und im Verteidigungsministerium; derzeit Leiter der Abteilung für Elektronische Abwehr/IKT-Sicherheit im Abwehramt

# CYBERCRIME:

## WAS KOMMT UND WAS BLEIBT

**Professioneller, kommerzieller, schneller: Die Trends der Internetkriminellen und Gegenstrategien**

*„Seit Jahren ist eine Professionalisierung und Kommerzialisierung der Internetkriminalität festzustellen. Die scheinbar unbegrenzten Möglichkeiten des Internet eröffnen, vor allem durch die Schaffung von Botnetzen, ein bisher nicht gekanntes Gefährdungspotenzial. Begünstigt durch das völlige Fehlen von nationalen Grenzen im Netz erfassen kriminelle Aktivitäten sehr rasch auch Österreich."*

Ministerialrat Mag. Leopold Löschl, BMI, Bundeskriminalamt, Leiter des Büros 5.2 Computer- und Netzwerkkriminalität



Im österreichischen Bundeskriminalamt ist das Büro 5.2 als Zentralstelle für die Bekämpfung der Computer- und Netzwerkkriminalität zuständig. Der rasante technische Fortschritt und die immer stärkere Verbreitung des Internet stellen dabei für die Ermittler eine ständig neue Herausforderung dar.

## Würmer wieder im Kommen

Schadprogramme wie Viren, Würmer und Spyware werden in immer kürzeren Entwicklungszyklen und in immer „optimierteren“ Varianten verbreitet. Im ersten Halbjahr 2009 ist die Infektion mit Computer-Würmern in Unternehmen im Vergleich zum Vorjahr weltweit um fast 100 % gestiegen. Prominentes Beispiel war der Virus Conficker, der bereits im November 2008 innerhalb von kürzester Zeit weltweit mehrere Millionen PCs infizierte.

## Gefahrenquelle gefälschte Antiviren-Software

Gefälschte Antiviren-Software ist als Gefahrenquelle auf dem Vormarsch. Sie ist darauf ausgelegt, den Benutzer zu verunsichern, indem Angriffe auf den Computer gemeldet werden, welche jedoch in Wahrheit nicht vorhanden sind. In einem weiteren Schritt wird die Bereinigung dieser Vorfälle angeboten. Nimmt sie der Benutzer gegen Bezahlung an, werden die Warnungen abgeschaltet oder der tatsächliche Angriff gestartet. In der ersten Jahreshälfte 2009 wurde diese Software von weltweit mehr als 13 Millionen Computern entfernt. Im Halbjahr davor waren es sogar 16,8 Millionen. Trotz des bemerkbaren Rückkangs ist hier weiterhin erhöhte Vorsicht geboten. Sicherheitssoftware sollte nur aus vertrauenswürdigen Quellen bezogen und ständig aktualisiert werden.

## Phishing – Totgeglaubte leben länger

Bis Mitte des Jahres 2007 sind die Meldungen von Phishing-Fällen ständig angestiegen. Danach war allerdings, entgegen den internationalen Trends, ein starker Rückgang feststellbar. Der Grund für diese positive Entwicklung dürfte neben polizeilichen Maßnahmen in einer Verbesserung der Sicherheitsvorkehrungen beim Online-Banking, bei Internet-Auktionen, Online–Games oder sozialen Netzwerken im Juni 2007 liegen.
Prominentestes Beispiel in Österreich ist wohl Online-Banking: Mit der letzten Bank in Österreich, die sich zum “Mobile TAN” durchgerungen hat, sind Phishing-Fälle massiv zurück gegangen. Maßgeblich dafür ist der zweikanalige Ansatz – Kanal 1: Internet (Web), Kanal 2: GSM-Netz (SMS) – dieses TAN-Systems. Dabei wird der Kommunikationsfluss zwischen Bank und Kunde auf zwei Kanäle entsprechend aufgeteilt, sodass es einem Angreifer so gut wie unmöglich ist, die finale Konto-Transaktion zu verfälschen. Die Gefahr beim Online-Banking in Österreich scheint damit vorerst gebannt zu sein. Wenn User allerdings beginnen, ohne nachzudenken alles zu bestäti-

gen, funktionieren diese Sicherheitsmechanismen nicht mehr.

## Mobile Gefahren

Der aktuelle technische Trend, täglich wiederkehrende Aufgaben in mobile Kleinstcomputer zusammenzufassen (Handy = Wecker = Browser = GPS = Mailclient = etc.), erhöht zwar Flexibilität bzw. Komfort enorm. Er bringt aber auch die große Gefahr mit sich, dass der beschriebene, sehr erfolgreiche Vorstoß in der Onlinebanking-Sicherheit wieder zunichte gemacht wird. Nutzt man sein Handy für Online-Banking, führt man damit die zwei getrennten Kanäle wieder zusammen und öffnet Attacken Tür und Tor. Es ist daher damit zu rechnen, dass früher oder später wieder eine Welle von Phishing-Angriffen auftreten wird.

Der Identitätsdiebstahl endet jedoch nicht beim Online-Banking. Obwohl es in diesem Bereich gelungen ist, das Problem mittelfristig reduzieren, geht es in anderen Bereichen weiter mit Account-Diebstählen. So hatte das Online-Spiel World of Warcraft mehrmals mit Phishing zu kämpfen. Durch den Diebstahl von Benutzerkonten und den Verkauf von virtuellen Gütern und Identitäten konnten die Täter Business generieren. World of Warcraft verteilt mittlerweile eine speziell konzipierte Hardware – ähnlich einem Schlüssel – an ihre Kunden, um die Kundendaten nicht mehr angreifbar zu machen.

## Conficker sorgt für Furore

Conficker, auch als "Downadup" oder "Kido" bezeichnet, ist eine Schadsoftware, die seit ihrem ersten Auftreten im November 2008 besonderes Aufsehen erregt hat. Conficker hat eine ganze Reihe von neuen Techniken mit schon bekannten intelligent verknüpft und somit innerhalb kürzester Zeit mehrere Millionen PCs infiziert.

In Österreich wurde Conficker erst bekannt, als die Kärntner Landesregierung am 8. Jänner 2009 mit diesem Problem an die Öffentlichkeit trat. Der Wurm legte ca. 3.000 Arbeitsplatzrechner lahm und sorgte dafür, dass Ämter tagelang offline waren. Auch ein Kärntner Spital wurde mit diesem Virus infiziert. Schlagzeilen wie “Krankenversorgung ohne EDV” verschafften dem Virus innerhalb kürzester Zeit auch in Österreich Berühmtheit.
Zu diesem Zeitpunkt erkannten erst wenige Antivirenhersteller eine bestehende Conficker-Infektion. Eine Ausbreitung zu verhindern schaffte keine einzige AV-Software.

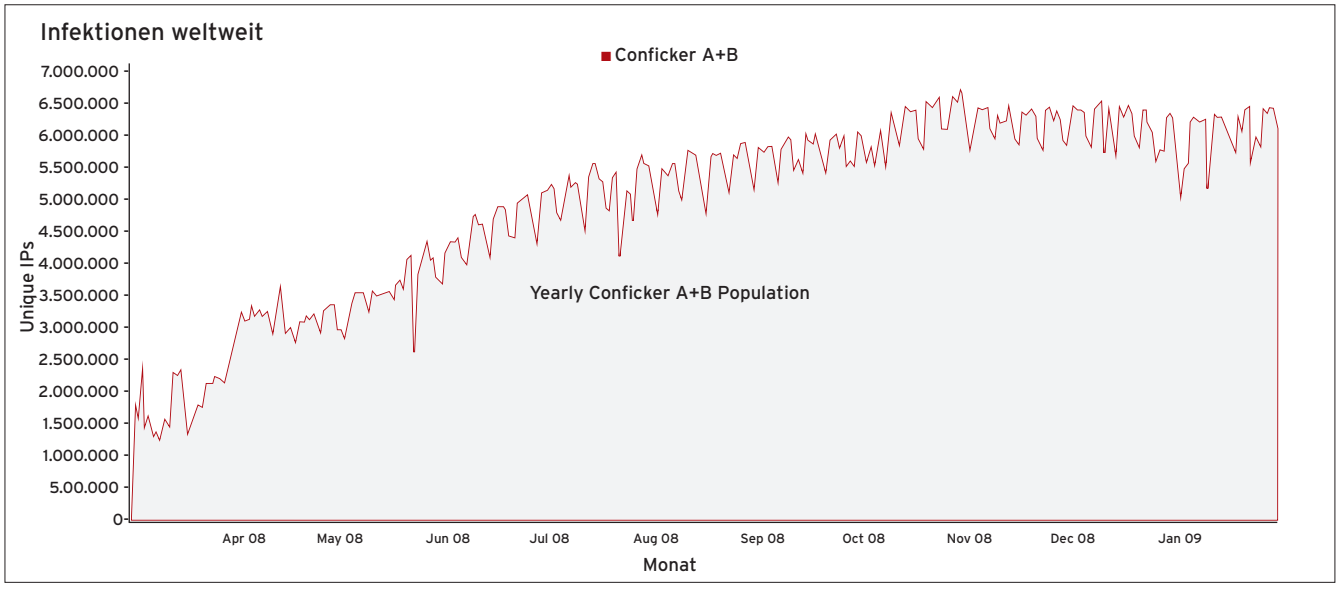



**Abbildung 5:** Anzahl der eindeutigen public IPs von Conficker.A und .B. Der Maximalwert beträgt ca. 6,5 Millionen. Quelle: Conficker Working Group



## Reaktionen und Incident Handling in Österreich

Sehr hilfreich war, dass eine Security-Interessentenrunde, zu der auch CERT-Experten sowie ein IT-Mitarbeiter der Krankenanstalt gehörten, rasch als Informationsdrehschreibe fungieren konnte. Innerhalb kürzester Zeit wurden Microsoft-Experten ausfindig gemacht, die sich des Problems vor Ort annahmen. Die Landesregierung und das Spital konnten durch gemeinsame Anstrengungen und in Wochenendschichten die mehreren tausend PCs bereinigen.
Es gab noch zahlreiche andere größere Unternehmen, bei denen Infektion, Erkennung und Bereinigung analog erfolgt sind.
Eine Gesamtquantifizierung des Schadens durch den entstandenen Arbeitsaufwand liegt nicht vor.

CERT.at konnte automatisiert Warnungen an die betroffenen Netzwerkbetreiber und Firmen senden und hatte somit die Gesamtübersicht, welche Netze in Österreich wie stark infiziert waren.

Die aktuellen Trends weisen darauf hin, dass die Verbreitung von Conficker.C abnimmt, aber Conficker.A und .B weiterhin stetig wachsen – und das selbst mehr als ein Jahr nach dem initialen Ausbruch.

Als besonders wertvoll im Sinne der Prävention erwies sich ein "Lessions-Learned"-Workshop, in dessen Rahmen IT-Verantwortliche aus der öffentlichen Verwaltung aus erster Hand von den Betroffenen über die Ereignisse, Probleme und Lösungsansätze informiert wurden. Diese Art von Informationsweitergabe im engsten Kreis wird stets von allen als besonders interessant bewertet, kann aber natürlich nur funktionieren, wenn auch die Bereitschaft besteht über Vorfälle zu sprechen und andere an den eigenen Erfahrungen teilhaben zu lassen.

Aktuelle Zahlen der Conficker Working Group zeigen deutlich, dass .A und .B noch eine große Gefahr darstellen. Und auch Conficker .C ist – wenn auch deutlich geschrumpft – immer noch ein großes Botnetz.

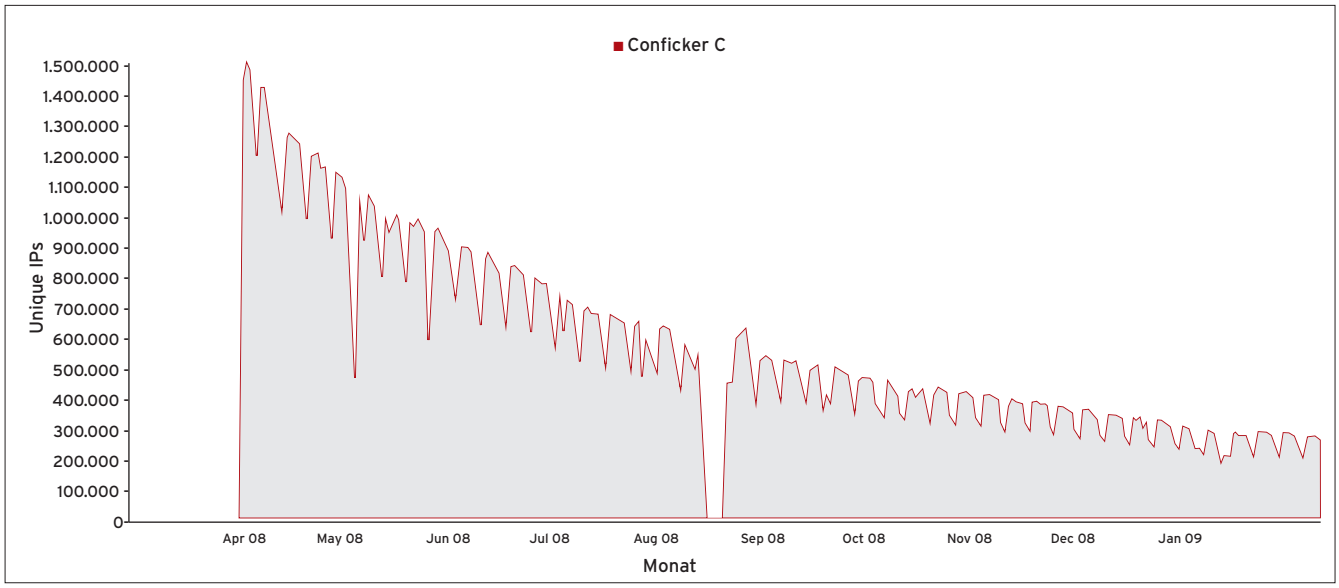



**Abbildung 6:** Anzahl der eindeutigen public IPs von Conficker.C. Quelle: Conficker Working Group

# HILFE ZUR SELBSTHILFE

## Ratschläge und Expertenhinweise zum besseren Schutz vor Cyberkriminalität

### Die Gefahr lauert immer und überall

Um Unternehmen vor Angriffen aus dem Cyberspace zu schützen, ist es wichtig, die notwendigen technischen Voraussetzungen dafür zu schaffen und optimal einzusetzen. Gleichzeitig muss aber auch das Bewusstsein der Mitarbeiter für Gefahrenquellen geschärft werden.

Der Einsatz von Virensoftware und einer Firewall nach außen reicht daher nicht aus, um ein Unternehmen wirkungsvoll zu schützen: Es bedarf eines durchdachten Sicherheitsplans.
Ausführliche Dokumentationen und Leitfäden zum Thema Schutz vor Risiken im IKT-Bereich gibt es seit Jahren in zunehmender Zahl, als einschlägige Standardwerke im deutschsprachigen Raum gelten z.B. die Veröffentlichungen des Bundesamtes für Sicherheit in der Informationstechnik www.bsi.bund.de. Als spezifisches Hilfsmittel für die inländische Wirtschaft und Verwaltung gibt es seit 1998 das regelmäßig überarbeitete und erweiterte Österreichische Informationssicherheitshandbuch, in das u.a. die Empfehlungen und Erkenntnisse der Koordinationsgremien der Plattform Digitales Österreich einfließen, und welches auch Verweise auf die relevanten gesetzlichen Bestimmungen enthält (www.asit.at/de/sicherheitsbegleitung/sicherheitshandbuch).

### Sicherheit in vier Stufen

**1) Vorsorgen statt Nachsehen**
Erster Schritt zum Schutz eines Unternehmens vor Cyberangriffen sind natürlich präventive Maßnahmen, die Viren, Würmer und andere Schädlinge schon am virtuellen Eingangstor zum Unternehmen abblocken. Klassischerweise passiert das durch eine Firewall. Zusätzlich empfiehlt sich, die Server in eine Demilitarized Zone (DMZ) zu bringen – ein Computernetz, in dem alle Zugriffsmöglichkeiten auf die daran angeschlossenen Server sicherheitstechnisch kontrolliert werden.
Firewall und Virenschutz sollten aber nicht nur nach außen abschirmen, sondern auch auf lokalen Endgeräten und Servern Schutz bieten.
Als genereller sicherheitstechnischer Grundsatz gilt: Alles, was nicht speziell erlaubt ist, ist verboten. Ein Beispiel: Die Nutzung von privaten USB-Geräten ist an Firmen-PCs nicht erlaubt und wird daher auch durch entsprechende technische Maßnahmen – z.B. durch entsprechende Konfiguration der Endgeräte – verhindert. Begleitet werden diese technischen Maßnahmen durch Warnung der Mitarbeiter vor den Tricks, mit denen Cyberkriminelle versuchen, unvorbereiteten Opfern sensible Daten zu entlocken. Dazu zählen geschenkte USB-Sticks, Anrufer, die vorgeben aus der IT-Abteilung zu sein und sich nach Passwörtern erkunden, Anfragen von angeblichen Mitarbeitern von Strom- oder Telekomanbietern etc.

**2) Rasches Erkennen möglicher Angriffe**
Prävention hilft nur so lange, bis sie fehlschlägt. Ein vollständiges Sicherheitskonzept enthält daher auch Maßnahmen, die der möglichst frühzeitigen Erkennung von erfolgreichen Angriffen dienen.
Aktuell sind das vor allem Intrusion Detection Systeme (IDS), die Sensoren an neuralgischen Stellen des Netzwerks besitzen und auf Angriffsmuster hin untersuchen. Auch die



Analyse der bereits im Unternehmen vorhandenen Daten (v.a. Log-Files) auf Auffälligkeiten gehört dazu. Viele Wurm-Infektionen lassen sich schon allein daran erkennen, dass auffällig viele ausgehende Verbindungsversuche von Endgeräten in den Log-Daten der Firewall oder auch Anfragen nach ungewöhnlichen Domains zu denen normalerweise keine Beziehung besteht in den Log-Daten des Nameservers auftauchen.
Antivirensoftware kommt schon bei der normalen Flut an Malware kaum nach. Man kann daher leider nicht davon ausgehen, dass sämtliche Schadsoftware von den Filtern geblockt wird. Das trifft noch in viel größerem Ausmaß auf gezielte Angriffe auf Organisationen zu: Wird Malware speziell für einen einzigen Einsatz geschrieben, haben die Filter kaum eine Chance, den Angreifer abzuhalten – der Erfolg des Angriffs ist so gut wie garantiert. Hier bleibt neben der erhöhten Aufmerksamkeit der Nutzer nur die ständige Suche nach verdächtigem Verhalten von infizierten PCs als Abwehrstrategie.

**3) Rasche Reaktion im Fall der Fälle**
Ein Sicherheitskonzept muss die rasche Reaktion auf Probleme durch Cyberangriffe vorsehen.
Von organisatorischer Seite her müssen folgende Punkte klar festgelegt werden:

- Wer ist zu verständigen?
- Wie sind die Ansprechpersonen zu erreichen?
- Wer ist wofür zuständig?
- Genaue Inventarisierung (auch im Notfall zeitnah verfügbar)
- Kommunikation bei IT-Totalausfall (eine Telefonanlage auf Voice-over-IP (VoIP)-Basis kann bei einem Totalausfall des IP-Netzwerks zum Beispiel unter Umständen nicht mehr für die Kommunikation/Koordination genutzt werden)

Dazu gehört auch das interne Telefonbuch und die Liste mit Nummern für Notfälle: Diese sollten auch auf Papier existieren.
- Einbindung externer Ressourcen
- Guideline für die externe Kommunikation

Von technischer Seite her sind folgende Punkte sicher zu stellen:
- Schadensbegrenzung
- Aufrechterhaltung/Wiederherstellung eines Notbetriebs
- Informationseinholung über alternative Kommunikationswege
- Wiederherstellung von Systemen
- Klare Priorisierung

**4) Lessons Learned**
Jeder Schadensfall sollte Anlass dazu geben, das Sicherheitskonzept nach Behebung aller Probleme anhand der aus dem Vorfall gelernten Lektionen zu aktualisieren und zu adaptieren.
Da aber allfällige Lücken und Mängel bei implementierten Präventivmaßnahmen nach Möglichkeit nicht erst in tatsächlichen Gefahrensituationen entdeckt werden sollten, besteht ein wichtiger Teil jedes Sicherheitskonzepts in der rechtzeitigen Durchführung von Tests und Simulationen. Diese werden auch im IKT-Bereich von vielen Organisationen teilweise schon seit Jahrzehnten auf regelmäßiger Basis intern durchgeführt – nachdem jedoch die Risikoquellen ebenso wie das World Wide Web selbst immer stärker vernetzt sind, ist auch in diesem Bereich eine höhere Ebene der Kooperation zunehmend erforderlich. Der bereits im Vorwort erwähnte Aktionsplan der Europäischen Kommission sieht noch für das Jahr 2010 die Abhaltung sowohl von nationalen als auch von europaweiten Notfallübungen vor, wobei an Hand verschiedener Katastrophenszenarien die Funktionsfähigkeit und vor allem die reibungslose Zusammenarbeit der diversen Schutzmechanismen und Institutionen getestet werden soll.

# CERT-ALPHABET

## Die wichtigsten Begriffe – kurz erklärt.

### Bot-Netz

Ein Bot (Abk. für Roboter) ist ein Programm, das auf dem PC eines Users installiert wird, ohne dass dieser es bemerkt. Der Besitzer des Bots kann dann aus der Ferne am fremden PC Anwendungen ausführen. Werden mehrere dieser virtuellen Roboter zusammengeschlossen, spricht man von einem Bot-Netz. Prominentes Beispiel für einen solchen Zusammenschluss von Bots ist Conficker.

### CERT

CERT ist die Abkürzung für „Computer Emergency Response Team“. CERTs sind Arbeitsgruppen oder Organisationen, die aktive Unterstützung bei IT-Sicherheitsproblemen in ihrem Verantwortungsbereich bieten. Das kann eine einzelne Organisation sein, in der das Team um den IT –Sicherheitsverantwortlichen die CERT-Rolle übernimmt, oder der Staat, wo das nationale CERT als Internet-Feuerwehr des Landes fungiert.

### Conficker

Conficker (auch bekannt unter Downup, Downadup, Kido und Worm.Win32/Conficker) ist ein Computerwurm für Microsoft Windows, der im November 2008 erstmals auftauchte und seither in mehreren Versionen aktiv ist. Er schaffte es Anfang 2009, weltweit die Windows-Netzwerke einiger kritischer Infrastrukturen zu infizieren.

### Demilitarized Zone

Eine Demilitarized Zone (DMZ, auch ent- oder demilitarisierte Zone) ist ein Computernetz mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die daran angeschlossenen Server. Die in der DMZ aufgestellten Systeme werden durch eine oder mehrere Firewalls gegen andere Netze (z.B. Internet, LAN) abgeschirmt. Durch diese Trennung kann der Zugriff auf öffentlich erreichbare Dienste (z.B. E-Mail, WWW, etc.) erlaubt, das interne Netz (LAN) aber gleichzeitig vor unberechtigten Zugriffen geschützt werden.

### DoS-Angriff

Denial of Service (DoS) heißt „außer Betrieb setzen“. Bei einem DoS-Angriff wird ein Computer von einer Reihe von anderen Rechnern mit Netzwerkpaketen oder Anfragen bombardiert. Die Folge: Der Rechner kann die gewaltigen Datenmengen nicht mehr verarbeiten und ist überlastet. Wird von mehreren Quellen her gleichzeitig angegriffen, spricht man von einem DDoS-Angriff (Distributed Denial of Service-Angriff).

### Estland- und Georgien-Vorfall

Im Frühjahr 2007 legten eine große Anzahl von DDoS-Angriffen estnische Webseiten von Unternehmen, Banken, Behörden, Polizei und Regierung tagelang lahm. Im Herbst 2008 passierte dasselbe mit georgischen Webseiten. Die Internetauftritte staatlicher Stellen in Georgien waren daraufhin nicht mehr aufrufbar.

### Firewall

Eine externe (Netzwerk- oder Hardware-) Firewall stellt eine kontrollierte Verbindung zwischen zwei Netzen her. Dabei überwacht die Firewall den durch sie hindurch laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden oder nicht. Auf diese Weise versucht die Firewall ein Netzwerk oder Netzsegment vor unerlaubten Zugriffen zu schützen.

### iTAN

Beim Indizierten TAN-Verfahren (iTAN) muss ein bestimmter TAN aus einer Liste angegeben werden. Der TAN ist dabei an einen bestimmten Auftrag gebunden und kann nicht für einen anderen Zweck verwendet werden. Ein geläufiges Beispiel dafür ist die TAN-Liste fürs Online-Banking.

### Lost Credentials

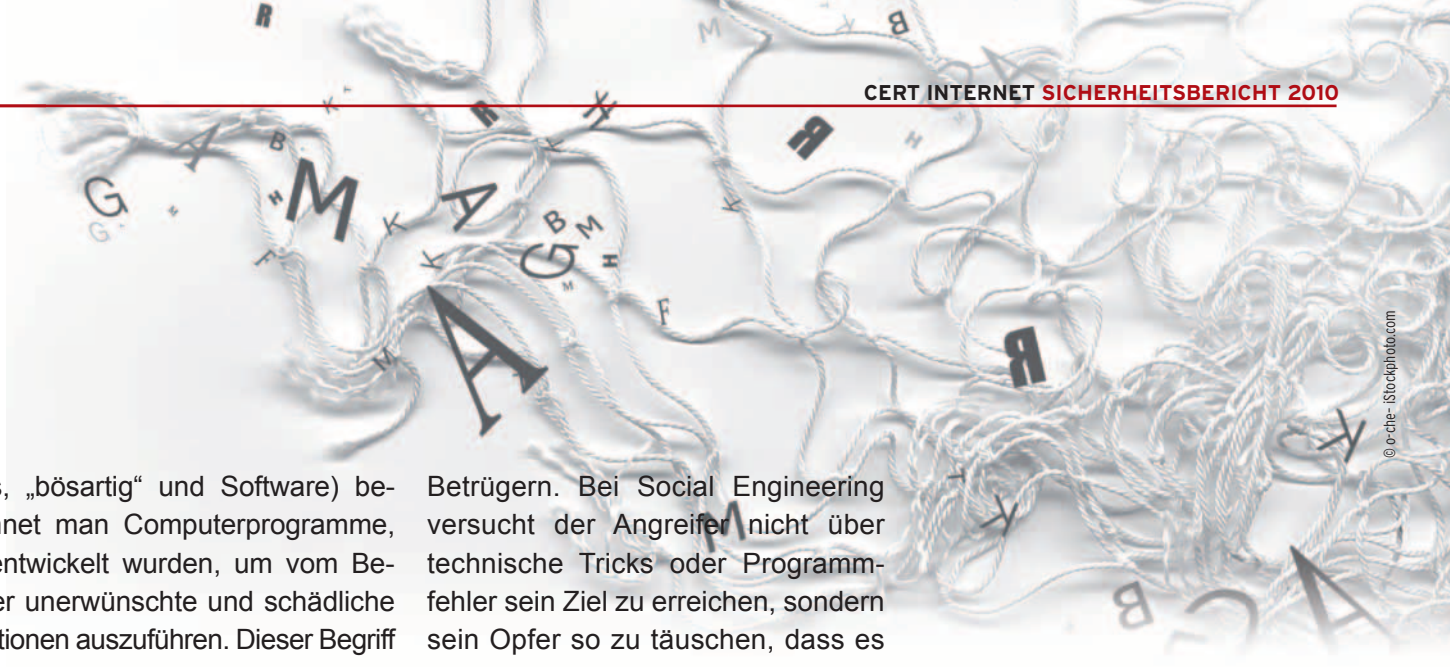
Unter diesem Begriff, der direkt übersetzt so viel wie „verlorene Berechtigung“ heißt, versteht man im Allgemeinen das unberechtigte Ausspionieren von Zugangsdaten und persönlichen Codes durch einen Autor von Schadsoftware.

### mTAN (auch smsTAN)

Mobile TAN (mTAN) oder auch smsTAN wird hauptsächlich im Online-Banking eingesetzt. Um eine Online-Überweisung erfolgreich abzuschließen, erhält der User einen Code via SMS, mit dem er das Bankgeschäft freigeben bzw. abschließen kann.

### Malware

Als Schadprogramm oder Malware (Zusammensetzung aus engl. mali-




cious, „bösartig“ und Software) bezeichnet man Computerprogramme, die entwickelt wurden, um vom Benutzer unerwünschte und schädliche Funktionen auszuführen. Dieser Begriff bezeichnet keine fehlerhafte Software, auch wenn diese Schaden anrichten kann. Malware wird von Fachleuten der Computersicherheitsbranche als Über-/Sammelbegriff verwendet, um die große Bandbreite an feindseliger, unerwünschter Software oder Programmen zu beschreiben. Als Malware Hosting bezeichnet man das Bereitstellen von Malware auf Webseiten.

### Man-In-The-Middle Attacke

Darunter versteht man den Angriff auf den Kommunikationskanal zwischen zwei oder mehreren Computersystemen. Dabei versucht der Angreifer, die Kommunikation unter seine Kontrolle zu bringen, ohne dabei bemerkt zu werden. Ziel ist es, den Informationsfluss einsehen und manipulieren zu können.

### Phishing

Der Begriff Phishing setzt sich aus „password“ und „fishing“ zusammen. Mit Phishing bezeichnet man den Versuch, mit Hilfe gefälschter E-Mails an vertrauliche Daten zu kommen. Oft funktioniert das über Webseiten, die den Loginseiten von Banken, Webmailservern oder anderen Webdiensten täuschend ähnlich sehen. Phishing ist eine bekannte Variante des „Social Engineering“.

### Social Engineering

Social Engineering meint im Zusammenhang mit dem IT-Security Thema eine bestimmte Strategie von Online-Betrügern. Bei Social Engineering versucht der Angreifer nicht über technische Tricks oder Programmfehler sein Ziel zu erreichen, sondern sein Opfer so zu täuschen, dass es von sich aus dem Angreifer hilft. Die Cyberkriminellen adressieren ihre Opfer bei dieser Methode oft individuell, und können so immer wieder Treffer landen. Surfgewohnheiten, Namen aus dem persönlichen Umfeld des Opfers etc. werden zuerst ausspioniert, um dann z.B. Phishing-E-Mails persönlich zu gestalten und das Vertrauen der jeweiligen Person gewinnen zu können.

### Spam

Als Spam bezeichnet man elektronische Nachrichten, die einem Empfänger unerwünschterweise zugestellt werden. Diese Nachrichten beinhalten oftmals werbliche Inhalte und werden in Massen versendet.

### System Compromise

Durch einen System Compromise verliert der eigentliche Besitzer des Systems die Kontrolle darüber. Dieser Kontrollverlust kann mehrere Gründe haben wie zum Beispiel die lückenhafte Kontrolle von Benutzerkennwörtern oder durchlässige Webapplikationen.

### Trojanisches Pferd

Als Trojanisches Pferd, auch kurz Trojaner genannt, bezeichnet man ein Computerprogramm, das als nützliche Anwendung getarnt ist, im Hintergrund aber ohne Wissen des Anwenders eine andere Funktion erfüllt. Ein Trojanisches Pferd zählt zur Familie unerwünschter bzw. schädlicher Programme, der so genannten Malware.

### URL Forwarding

URL Forwarding (zu Deutsch „Domainweiterleitung“) ist prinzipiell nichts Verbotenes und wird verwendet, um den User beim Eintippen einer Domain in den Browser zu einer anderen Domain weiterzuleiten, beispielsweise von .at zu .com. Diese Weiterleitung kann jedoch auch, obwohl sie auf den ersten Blick unverfänglich aussieht, zu einer Website führen, die den Benutzer dazu auffordert, Antischadsoftware downzuloaden. Das Resultat ist die Installation der eigentlichen Schadsoftware.

### Website Defacement

Mit Website Defacement (oder auch nur Defacement) wird die unberechtigte Veränderung einer Website bezeichnet. Dabei werden Sicherheitslücken ausgenützt oder gestohlene Passwörter benutzt, um das visuelle Erscheinungsbild einer Website zu „entstellen“. Oftmals wird auch eine Botschaft auf der veränderten Website hinterlassen. Einer der berühmtesten Fälle war wohl das Hacken der Webpräsenz des CIA in den 1990er Jahren.

**MEHR INFORMATIONEN UNTER**
**WWW.CERT.AT**
**UND**
**WWW.GOVCERT.GV.AT**

**WIEN 2010**