



## PROBEABONNEMENT DCERT-INFOSERVICE

Interessenten erhalten ein kostenfreies 4-wöchiges Probeabonnement des dCERT-Infoservice. Anmeldungen sind unter [www.dcert.de](http://www.dcert.de) möglich.

# DCERT – IHR WEGWEISER DURCH DIE IT-SECURITY.

## WACHSENDE PROFESSIONALITÄT VON CYBERANGRIFFEN.

Die Bedrohung von Know-how und Geschäftsbetrieb durch Angreifer aus dem Cyberspace hat stark zugenommen. Wo früher Einzeltäter oft ideologisch motiviert agierten, sind Angreifer heute wesentlich komplexer und professioneller organisiert. Ihre Angriffe sind kriminell oder politisch motiviert und reichen von Datendiebstahl über Wirtschaftsspionage bis hin zum Cyberwar zwischen Staaten.

Dabei bedienen sie sich der Schwachstellen in Software und Netzwerken, von denen täglich neue entdeckt und auf regelrechten Märkten im Internet gehandelt werden. Über diese Schwachstellen dringen sie in fremde Systeme ein und suchen nach Kundendaten, Entwicklungsergebnissen oder Betriebsgeheimnissen – kurz allem, was sich zu Geld machen lässt oder dazu dient, die Konkurrenz auszustechen. Allein die Deutsche Telekom registriert binnen 24 Stunden rund 100.000 Angriffe aus dem Internet auf ihre Systeme.

Die Möglichkeiten der Angriffe sind sehr vielschichtig: Sie reichen von Identitätsdiebstahl über das Einschleusen kompromittierender Hard- oder Software, die bewusst fehlerhaft arbeitet oder eine Fremdsteuerung erlaubt bis hin zu Denial-of-Service-Attacken, die Server oder Geschäftsprozesse lahm legen.

## ANGREIFER AGIEREN WELTWEIT.

Der Schaden, den Cyberangriffe jedes Jahr verursachen, beläuft sich laut dem Norton Cybercrime Report des Sicherheitsunternehmens Symantec auf knapp 400 Milliarden Dollar. Nach einer Studie des Sicherheitsspezialisten McAfee waren Unternehmen, die sich mit der Versorgung von Strom, Öl, Gas und Wasser beschäftigen noch nie so gefährdet wie heute. 80 Prozent der befragten Betriebe wurde bereits angegriffen, ein Viertel von ihnen erpresst.

# TAGESAKTUELLE INFORMATIONEN ZU SCHWACHSTELLEN IN DER IT – INKLUSIVE SCHADENS- POTENZIAL UND HANDLUNGSEMPFEHLUNGEN.

## INFORMATIONEN ALS WAFFE GEGEN ANGREIFER.

Um Gefahren frühzeitig zu erkennen und Sicherheitsmaßnahmen zu entwickeln, hat T-Systems mit dCERT einen Cyber-Defense-Informationssdienst aufgebaut. Kern des Dienstes ist die Analyse, Bereitstellung und Dokumentation von Informationen zu unternehmensrelevanten Bereichen der IT-Sicherheit. Das dCERT-Team recherchiert täglich in einschlägigen Quellen und erhält durch die Mitgliedschaft im Forum of Incident Response and Security Teams (FIRST) sowie durch die enge Zusammenarbeit mit Notfallteams in aller Welt Zugang zu vertraulichen Hintergrundinformationen. Jährlich analysieren und beschreiben die Security-Spezialisten rund 1.200 Meldungen zu neuen IT-Schwachstellen und bewerten deren Relevanz für Unternehmen. Kunden des dCERT-Infoservice, zu denen neben der Deutschen Telekom auch Banken und Servicedienstleister im Finanzbereich sowie Logistikunternehmen gehören, bekommen täglich aktuelle Informationen zur IT-Sicherheit per E-Mail und können alle bisherigen Meldungen in der Online-Datenbank recherchieren. Verweise auf die Originalmeldungen machen die Bewertungen transparent und nachprüfbar.

Das dCERT-Team empfiehlt zudem Lösungen für akute Bedrohungen. Es verweist auf Patches und Updates der Hersteller oder Workarounds, um die Gefahrenstelle zu umschiffen. Angaben zur Eintrittswahrscheinlichkeit und potenziellen Schadenshöhe helfen, die Bedeutung einer Schwachstelle für das jeweilige IT-System zu erkennen.

### DAS WICHTIGSTE AUF EINEN BLICK.

- Security-Spezialisten des dCERT-Teams recherchieren, bewerten und dokumentieren Informationen zu Schwachstellen in IT-Systemen.
- Kunden erhalten täglich einen E-Mail-Bericht zur aktuellen Bedrohungslage (dCERT Advisory).
- Unter [www.dcert.de](http://www.dcert.de) stehen sämtliche bisherigen Meldungen zur Recherche bereit, ergänzt um statistische Auswertungen.
- Premiumkunden erreichen das dCERT über eine Notfallrufnummer.
- Bei einem Sicherheitsvorfall beraten die Security-Experten Kunden und empfehlen Gegenmaßnahmen.

## LEISTUNGSUMFANG DES DCERT-INFOSERVICE.

### Tägliches Update per dCERT Advisory

Abonnenten des dCERT-Infoservice erhalten werktags um 14 Uhr aktuelle Informationen zur IT-Sicherheit (dCERT Advisory). Die Meldungen werden signiert per E-Mail übermittelt und stehen im CVRF-Format oder anderen Formaten zur Verfügung. Monatlich erfolgt eine Zusammenfassung aller Meldungen. Mit dem Abonnement erhalten Kunden Nutzungsrechte für das gesamte Unternehmen.

### Online-Recherche

Kunden können alle veröffentlichten Meldungen seit Start des Dienstes im Dezember 1999 in der Onlinedatenbank recherchieren und in vollem Umfang einsehen.

### Statistik

dCERT aktualisiert täglich Statistiken zur Meldungsanzahl oder zur Kritikalität der Meldungen über einen Zeitraum von 18 Monaten. Kunden können diese Grafiken für eigene Auswertungen verwenden.

## ZUSÄTZLICHE LEISTUNGEN DES DCERT-TEAMS.

### Notfallnummer

Premiumkunden erreichen Mitarbeiter des dCERT während der Geschäftszeiten über eine Notfallrufnummer. Am Wochenende und an Feiertagen wird ein Rückruf innerhalb von 24 Stunden garantiert.

### Sicherheitsseminare

Für einen vertiefenden und individuellen Austausch zu allen Themen der IT-Sicherheit bietet das dCERT-Team auf Wunsch Analystentage oder Seminare zu ausgewählten Themen der IT-Sicherheit.

### Individuelle Beratung bei Sicherheitsvorfällen

Im Schadensfall berät das dCERT-Team seine Kunden und unterstützt bei der Eindämmung und Beseitigung der Schäden.

### HABEN SIE NOCH FRAGEN?

Dann kontaktieren Sie uns  
Internet: [www.dcert.de](http://www.dcert.de)  
E-Mail: [info@dcert.de](mailto:info@dcert.de)  
Telefon: +49 228 9841-5500

### EXPERTENKONTAKT

T-Systems International GmbH  
Günter Kreuzer  
Deutsche Telekom-Allee 7  
64295 Darmstadt

### HERAUSGEBER

T-Systems International GmbH  
Hahnstraße 43d  
60528 Frankfurt  
Deutschland