DCERT – YOUR GUIDE TO IT SECURITY.

GROWING PROFESSIONALIZATION OF CYBERATTACKS.

Cyberattack risks for companies' intellectual property and business operations have been growing sharply. While attackers of yore were often ideologically motivated individuals, modern attackers tend to be part of complex, professional organizations. Their attacks, which can be either criminally or politically based, can have a range of aims, from data theft to industrial espionage – or even the advancement of cyberwar between states.

Attackers exploit weaknesses in software and networks. New such weaknesses are discovered every day, and the keys to such weaknesses are traded in what has developed into a proper marketplace on the Internet. Using such weaknesses, attackers penetrate into systems and search for customer data, development results and operational secrets – in short, anything that they can sell, or use to the competition's disadvantage. Within the space of a 24-hour period, Deutsche Telekom registers some 100,000 Internet-based attacks against its systems.

Attackers can pursue a wide range of specific agendas, including identity theft via the injection of malware for purposes of sabotage or external control; and denial-of-service attacks that can paralyze servers and business processes.

ATTACKERS WORK ON A GLOBAL SCALE.

According to the Norton Cybercrime Report by security solutions provider Symantec, cyber attacks cause some 400 billion dollars' worth of damage every year. A study by security specialists McAfee found that companies in the power grid, oil, gas and water industries are more vulnerable today than ever before. 80 percent of enterprises surveyed had already fallen victim to an attack, and a quarter had been blackmailed.

T · · Systems ·

DAILY UPDATES ON IT VULNERABILITIES – INCLUDING POTENTIAL DAMAGE AND RECOMMENDED ACTION.

INFORMATION AS A WEAPON AGAINST ATTACKERS.

T-Systems has developed dCERT, a cyber-defense-information service, with a view to supporting efforts to detect threats early and to develop appropriate security measures. The core services provided by dCERT include analysis, provision and documentation of information relevant to important areas of corporate IT security. On a daily basis, the dCERT team monitors relevant newsgroups and web forums. In addition, via its membership in the Forum of Incident Response and Security Teams (FIRST), as well as through close cooperation with emergency-response teams throughout the world, it has access to relevant confidential background information. Every year, security specialists register around 1,200 reports relating to new IT vulnerabilities. These are analyzed and evaluated in terms of their relevance to business. dCERT-Infoservice customers – along with Deutsche Telekom, they include banks, financial service providers and logistics companies – receive e-mails with current information on IT security every day. In addition, they have access to an online database, which contains all previous reports. Links to the original reports are included for the sake of transparency and verifiability.

The dCERT team also recommends solutions to acute threats. It reports on manufacturers' patches and updates, as well as on useful workarounds for specific risks. Additional information about probabilities of occurrence, and the magnitude of potential damage, help subscribers to assess the importance of specific weaknesses with regard to their own IT systems.

THE MOST IMPORTANT INFORMATION AT A GLANCE.

- Security specialists of the dCERT team gather, assess and document information about weaknesses in IT systems
- Customers receive daily e-mail reports (dCERT Advisories) about the current threat situation
- At www.dcert.de, subscribers have access to an archive with all past reports, supplemented by statistical analyses.
- Premium customers can contact dCERT via an emergency phone number.
- In the event of security incidents, the service's security experts advise customers and recommend countermeasures.

SERVICES INCLUDED IN THE DCERT-INFOSERVICE.

Daily update: the dCERT Advisory
Every weekday, beginning at 2 p.m., dCERT-Infoservice subscribers receive current information on IT security (the dCERT Advisory). Reports, which are sent via signed e-mail, are available in a range of formats, including CVRF. Each month, subscribers receive a summary of the month's reports. By subscribing to the service, customers receive usage rights that are valid for their entire company.

Online research
Customers receive full access to an online archive with all reports published since the service was launched in December 1999.

Statistics
dCERT updates its statistics on the numbers of reports and on the criticality of reports on a daily basis, over an 18-month period. Customers are free to use the relevant diagrams for purposes of their own analyses.

ADDITIONAL SERVICES OF THE DCERT TEAM.

Emergency phone number
Premium customers get access to an emergency phone number which they can use to reach dCERT staff during business hours. For calls on weekends and holidays, dCERT guarantees callbacks within 24 hours.

Security seminars
Upon request, the dCERT team offers meetings with analysts and seminars on selected IT-security topics. Such events provide opportunities for in-depth, one-on-one exchanges relative to all aspects of IT security.

Individual support in connection with security incidents
In cases of damage, the dCERT team advises customers and provides assistance in containing and eliminating damage.

ANY QUESTIONS?
Then contact us!
Internet: www.dcert.de
E-mail: info@dcert.de
Phone: +49 228 9841-5500

TO CONTACT EXPERTS
T-Systems International GmbH
Günter Kreuzer
Deutsche-Telekom-Allee 7
64295 Darmstadt, Germany

PUBLISHED BY
T-Systems International GmbH
Hahnstr. 43d
60528 Frankfurt
Germany