

Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology
Herausgeber: Swisscom
Band: 83 (2005)
Heft: 6

Artikel: Cybersecurity : an issue for all
Autor: [s. n.]
DOI: <https://doi.org/10.5169/seals-877157>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. [Siehe Rechtliche Hinweise.](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. [Voir Informations légales.](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. [See Legal notice.](#)

Download PDF: 15.03.2025

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

Cybersecurity – an Issue for all



The cyberworld is open to very similar threats to the real world: theft, racketeering, vandalism, exploitation, extortion, fraud and terrorism.

Spam, viruses, worms, identity theft or phishing, Trojans and denial of service all combine to make the issue of cybersecurity a serious one. As computers and the Internet are now inseparable parts of daily life, the need for effective security measures to protect the computer and telecommunication systems is imperative.

And, with today's mobile phones replicating the functionality of personal computers (PC), mobile networks are increasingly susceptible to malicious attacks. A successful attack on a mobile network has the potential to be very damaging, given that the mobile phone subscribers worldwide far outnumber PC users. ITU estimates that in mid-2005, there were around 2 billion mobile phones worldwide, compared with about 750 million Internet users.

The Internet has opened up legitimate new trade routes and opportunities for thousands. However, it has also be-

come a trading place for anything from pirated music and film to programs that allow the defrauding of companies by – other – electronic means. As well, the Internet has made cross-border fraud infinitely easier, which makes prosecution and investigation complicated.

ITU is increasing awareness of cybersecurity issues among stakeholders. For example, the ITU WSIS Thematic Meeting on Cybersecurity, held in Geneva from 28 June to 1 July 2005, underscored the importance of sharing information on national approaches:

- good practices and guidelines
- developing warning and incident response capabilities
- harmonising national legal approaches and international legal coordination
- technical standards
- privacy, data and consumer protection
- and providing assistance to developing countries

Dangers in the Cyberworld

With such a huge focus on implementing the most advantageous IT solution or determining which of the latest and greatest Web applications, servers and databases best suits the mission of an organisation, protecting the information held by those assets has often been a second priority. Many enterprises may be fooled into thinking that, because they have not been hit, there is no threat. Not so. The cyberworld is open to very similar threats to the real world: theft, racketeering, vandalism, exploitation, extortion, fraud and terrorism. The recording industry, for example, is working hard to combat downloading of its wares from file sharing networks.

Spam

Statistics from MessageLabs, a global company that provides managed e-mail security services to more than 9000 businesses worldwide, show that of the 12.6 billion e-mails it scanned during 2004, a whopping 9.2 billion (or 73.2%) were identified as spam. These statistics were brought live during the Cybersecurity Symposium II organized jointly in Moscow in March 2005 by the ITU Telecommunication Standardisation Sector (ITU-T) and the Russian Association for Networks and Services (RANS). They show that the overall trend during 2004 was an increase in spam volumes, with sharp peaks in June and July.

Some of the arrests that have been made since the introduction of anti-spam laws around the world have been important in demonstrating that spamming is a crime that will be dealt with. The Australian Spam Act that went into effect in April 2004 is often cited as one of the most successful spam laws to date. This Act imposes fines of up to US-\$ 1.1 million a day until a spammer stops. The most determined, however, transfer their business to countries where no legislation exists.

Viruses

Another threat to computer systems has come from viruses. While most have contained relatively innocuous payloads, the potential exists for them to be damaging on a wide scale. The "I love you" virus that struck in the year 2000 offers an example of this. The year 2004 began with a bang when the first of the "MyDoom" worms entered the scene, followed by many variants of particular viruses. Of the 147 billion e-mails scanned by MessageLabs during 2004, about 901 million (or 1 in 16) contained a virus. The chart on CanCert Networks in Canada shows how these attacks on networks are increasing.

Why this continual stream of reincarnated viruses and worms? One reason is that a virus code is often released into the public domain, making it easy for copycats to use as the basis of their own creations. Another is that virus writers are aware of the window of vulnerability, and know that they have a period of time during which no software-based protection exists against new malware. They take advantage of this by creating a malicious code designed to spread far and fast, thereby infecting the greatest number of machines. For the anti-virus software vendor it is back to the drawing board, and so the cycle continues.

Virus attacks can usually be traced to exploitation of one

of a small number of security flaws. And a simple policy of ensuring that all systems are kept up to date with the latest security patches and users are aware of some simple security rules will thwart the majority of these attacks. An additional deterrent for virus writers is a tough legal policy.

But insider attacks are almost certainly more common and have the potential to be much more damaging. ITU-T Recommendation X.800 lists a number of protection methods that can be used against such attacks.

Phishing

Phishing e-mails are those fraudulent notes that scam artists send you asking you to confirm your credit card data. Phishing attacks became the major threat of 2004, with a wave of them targeting individual or small groups of companies specifically. This has put business on the front line in the fight against online attacks.

Viruses and spam have dominated the e-mail landscape as the two main security threats faced by businesses. And just as the convergence of the two began to present a real potent threat, another equally sinister threat in the name of "phishing" was in the making. In September 2003, MessageLabs intercepted 279 phishing e-mails (e-mails containing a URL to a fraudulent website). That figure had risen to over 2 million by September 2004. So, in just twelve months, phishing had become a threat to any organisation or individual conducting business online. During 2004, the company intercepted over 18 million phishing e-mails. No wonder it dubbed 2004 "the year the big phish was landed".

Typically, phishing attacks require users to click on a URL within an e-mail, which appears to have come from a legitimate bank or e-commerce site, then enter personal account details into a fraudulent website, putting them at risk of identity theft.

Then came the phishing e-mails designed to capture online banking details automatically when a computer user opens the e-mail as opposed to when the user clicks on the URL link.

In another twist, phishers attempt to recruit middlemen by luring unsuspecting users into money-laundering operations and exposing them to possible identity theft. They offer these potential victims positions with a legitimate organisation whose name is used in an attempt to lend credibility to the scam.

Phishing incidences are reported to have reached a peak in January 2005, dropped but then shot up again in May 2005, exceeding anything seen before. Security experts are attributing this to the huge rise of zombie botnets being used to pump out massive volumes of the scam e-mails, as cybercriminals look to increase their profits.

Apart from the rise in phishing, virus and spam volumes, tailored malicious activity range from denial of service attacks targeted at blackmailing online gaming sites to threats that send out child pornography in the name of a particular reputable organisation.

A Standards Solution

Standardisation provides a solid way of coordinating resources to fight cybersecurity threats. ITU-T provides an

international platform for the development of the protocols that will protect current and next-generation networks. At present, all 13 ITU-T study groups are looking at security-related questions, and regular security workshops invite non-member participants to contribute to a road map for future work and coordination between other standards-development organisations.

A recent example of a standard addressing security concerns followed industry demands for a new approach to assessing security risks in networks. ITU-T Recommendation (X.805) will give telecommunication service providers and enterprises the ability to provide an end-to-end architecture description from a security perspective. The Recommendation will allow operators to pinpoint all vulnerable points in a network and address them. Incorporating X.805 into a risk-management policy will give the network owner the confidence to be able to say that it has addressed security issues to the best of its ability.

There are over seventy ITU-T Recommendations focusing on security. ITU-T's work on security covers a wide area. Work includes studies into: security from network attacks, theft or denial of service, theft of identity, eavesdropping, telebiometrics for authentication, security for emergency telecommunications and telecommunication networks security requirements.

In fact, one of the most important security standards in use today is X.509, an ITU-T developed Recommendation for electronic authentication over public networks. X.509 is the definitive reference for designing applications relat-

ed to Public Key Infrastructure (PKI). The elements defined within X.509 are used widely, from securing the connection between a browser and a server on the Web to providing digital signatures that enable e-commerce transactions to be conducted with the same confidence as in a traditional system. Without wide acceptance of the standard, the rise of e-business would have been impossible.

Standards for Next-Generation Networks

Recommendation H.235 provides the protocols necessary for IP media such as voice over Internet Protocol (VoIP) or videoconferencing calls to be authorized and routed. With the help of H.235, users communicating through IP media are authenticated and authorized so that their communications are protected against various security threats. Real-time multimedia encryption adds a further layer of security, protecting against call interception. The security countermeasures are designed to thwart service fraud, avoid service misuse and detect malicious message tampering. H.235 also gives the ability to provide a greater level of security using PKI certificates. In addition to this standard, ITU-T's multimedia Study Group has started work on a standard that will allow VoIP and other IP-based protocols to be more easily implemented in a secure enterprise or service provider environment. ■

Sources: ITU

Info: ITU, Place des Nations, 1211 Geneva 20, Tel. 022 730 52 34, itunews@itu.int, www.itu.int

Suchen, senden, finden

I-SEARCH – vielseitig einsetzbar

Wenn es um das Benachrichtigen von mobilen Personen geht, kennt I-SEARCH keine Grenzen. Egal, ob eine Person im Haus, auf dem Betriebsgelände oder unterwegs ist – mit I-SEARCH informieren Sie Ihr Personal zielgerichtet! Die Übermittlung von Textbotschaften erfolgt über Pager, Handy oder E-Mail. Eine Anbindung an DECT Systeme ist ebenfalls möglich. I-SEARCH lässt sich darüber hinaus in jedes TVA- bzw. IT-Umfeld integrieren.



www.swissphone.ch

SWISSPHONE