CYBER SECURITY
INDUSTRY ALLIANCE

Securing Data under the Proposed EU Data Retention Draft Directive

December 2005

The European Parliament and Council of the European Union are poised to adopt a major Directive calling for data processed by public electronic communication services to be retained. The data would include “traffic and location data”, such as information about the source and destination of the communication (names and addresses, telephone numbers, IP addresses, time and duration of the communication, and communication device used). The proposed Directive is particularly aimed at a new generation of electronic communications services based on the Internet Protocol, and designed to assist law enforcement, in the fight against terrorism.

Substantial debate has ensued over issues such as protecting the privacy of individuals identified by retained traffic data, and meeting the financial costs required by service providers to retain the data. This policy briefing addresses a different critical aspect of the Directive: ensuring the cyber security of traffic and location data stored by service providers.

It is the Cyber Security Industry Alliance’s (CSIA) position that no matter what sort of data is retained or how long it is held, all data should be properly secured. European legislators and officials should carefully consider provisions for the security of the stored traffic data. Without systematic protective measures, ensuring the privacy of EU citizens will be difficult. Including data security provisions in the Directive will also help control the total lifetime costs of information technology required to safely store and use traffic data by law enforcement.

This document was prepared by the Cyber Security Industry Alliance. CSIA is a global private industry advocacy group for enhancing cyber security. Its members represent the world’s leading providers of cyber security technology. Members of CSIA work closely with governments worldwide to help protect information security and the resilience of critical IT operations.

Contents

ISSUE SUMMARY

Databases are Vulnerable to Attack

Database applications use the Internet for transmitting and receiving data. Their very presence on the Internet exposes them to an ever-rising tide of malicious software, or "malware", and potential unauthorized exploitation. Automated hacking tools bring IP-connected databases under constant attack. Experts no longer track the gross volume of cyber security incidents because they literally occur on a non-stop basis. Service providers will be required to employ best practices for cyber security and use state-of-the-art technology solutions to protect traffic data stored under the proposed Directive.

Data Retention Increases the Risk of Breach

Various lengths of time for the retention of data have been considered, depending on the nature of the data. Regardless of the length of time the data is retained, the mere retention of the data implies potential risks. These risks increase over time and proportionally with the size of the database and the amount of data stored. The retention of data increases the risk of deliberate or accidental exposure of personal information.

Breaches will occur without Systematic Cyber Protection

The interconnected, web-like nature of the Internet increases a database's potential points of exposure to malicious software and other external sources of exploitation. In addition to outside threats, Member States will need to ensure that service providers and other holders of data protect the stored traffic data from exposure or exploitation by unauthorized insiders, including employees, business partners, contractors – and government workers. Adequate protection will require systematic planning and implementation of cyber security provisions throughout all organizations storing and using the databases.

CYBER RISKS TO DATABASES

In this age of cyber crime rings and information thieves, a database containing a person's private information is a gold mine. The re-sale of banking data, credit card numbers and other personal information has become big business in online marketplaces run by cyber criminals. Similarly, the use of traffic data could be exploited by unscrupulous entities seeking to track and misuse the stored communication data. Databases at many European companies have incurred breaches by hackers and unethical employees. More than 80 percent of 200 large-scale British businesses surveyed in 2005 reported being the victim of unauthorised access to their data networks, according to Britain's National Hi-Tech Crime Unit.[1] Many noted sabotage of data networks by company insiders as a key concern, so all companies,

[1] Source: National Hi-Tech Crime Unit 2005 e-crime survey; see www.nhtcu.org/media/documents/Press_Releases/2005/e-crime_Costing_British_Business_Billions_050405.pdf.

even those with large information technology budgets are at risk. New databases of personal communications traffic data will add a significant attractive target to criminals or organizations with malicious intent.

External Cyber Risks

A simple web search for "keylogger" or "port sniffer" can lead a hacker to readily-available software tools that help crack access to confidential databases on the Internet. These programmes can be silently installed on a computer system to record key strokes or probe for vulnerable networks and databases. Observers say more than 6,100 new keylogger programmes are now available on the Internet. [2]

These programmes and other spyware are used by organised criminals to anonymously record user names, passwords and credit card details. Unprotected databases are vulnerable to exploitation by users of these programmes. During 2005, major banks, information vendors and telecommunications firms have all been hit by such information thieves.[3] Exploitation of an unprotected network or database is not difficult for a hacker with even basic skills.

Another way malicious outsiders exploit vulnerabilities is through misconfigured security protocols. A common mistake is leaving a system's default password and username setting unchanged. "Admin" and "password" are often the first guesses a hacker will try in attempting to access a system. A hacker who achieves un-authorised system administrator status can exploit virtually any aspect of the network or database.

Cyber Risks Exploited by Insiders

Stealing confidential information from a database is easy for an insider with authorised access to the network and database. Insiders include co-workers, contractors, business partners, or any person with authorized access to protected data. People who are terminated from employment are another potential point of risk if they have retained copies of protected data, or have continued access to the system and valid passwords after they leave their employer. Not only cyber security technologies but best practices for information usage are required to counter these insider risks.

Carelessness is another cause of security breaches. An employee may accidentally attach a confidential file and email it to an unauthorized recipient outside the company. Employees might lose a laptop computer, hard drive, or CD-ROM that contains protected data. Many organisations recycle up to 70% of old hard disks – some of which contain information or applications that provide access to a network and secured files.[4] This vulnerability could be erased with a practice of "clean wiping" all recycled disks prior to redeployment.

Other common but hazardous cyber security practices include lax controls over who has access to the network and databases, and inadequate controls governing transfer

[2] iDefense, 15 November 2005. http://www.idefense.com/about/newscenter/recentreleases/2005_11_15.jsp?flashstatus=true.

[3] 2005 Global Security Survey, Deloitte Touche Tohmatsu, http://www.deloitte.com/dtt/research/0,1015,sid%253D2211%2526cid%253D86575,00.html

[4] Source: Prof. Urs E. Gattiker, technical director of CyTRAP Labs; interview 18 November 2005.

of protected information to a second PC or to a personal handheld computing device. Some organisations are unable to ascertain who has accessed secure areas of a network or database, when they gained entry, and what they did once they were in.

SOLUTIONS FOR PROTECTING DATABASES

Applying security best practices is crucial for preventing breaches of stored data. Encouraging a voluntary system of harmonised best practices across the European Union would lessen the compliance burden on everyone that maintains commercial databases within the EU and abroad. Information security can be provided through the combination of appropriate physical, administrative and technological safeguards. These safeguards may include intrusion detection, authentication and access controls, encryption, and monitoring capabilities, which are described in more detail below.

Intrusion Detection

Networks and servers hosting databases should use up-to-date firewalls, and intrusion detection and prevention software. Perimeter defenses such as firewalls have been recognized by industry as the absolute minimum cyber security protection and are seen as the starting point for a properly secured system. Installing intrusion detection technology on the database itself, as opposed to only on the network is also a valuable tool.

Authentication and Access Controls

Authentication is a process whereby a person or computer program proves their identity in order to access information. Proof of identity is generally given through: something the user ***knows*** (such as a password); something the user ***has*** (such as a smart card or electronic token); or something the user ***is*** (such as a biometric characteristic, like a fingerprint). “Strong” authentication requires at least two of these elements.

Once a user has been authenticated, access controls determine what privileges that user enjoys. Different levels of privileges, or users’ rights, can be provided, and a given user may be granted some of these privileges but not others.

Encryption

Encryption technologies can make it virtually impossible for unauthorized people to read data. Encryption obscures the data and requires a “key” to transform it back into a readable format. Encryption is another way to limit access to information to those people or departments that are authorised to have that access regardless of whether data is in transit, in use or in storage. Databases with personal traffic data should be properly encrypted.

Monitoring

Conducting regular penetration tests and audits of the database to monitor any changes to database security rights is imperative. Knowing who accessed the information when, where and for what purpose is essential for demonstrating that an organisation has taken appropriate steps to mitigate cyber threats.

Monitoring is particularly important for knowing which data has been accessed and if and where the data has been transferred, for example to employee computers, mobile computing devices, or to external recipients. Data is frequently transferred in healthcare, where patient records are exchanged between doctors. Data is also frequently transferred between multiple law enforcement agencies. Monitoring is one way of ensuring that data is properly shared when different organisations are collaborating.

ECONOMIC VALUE OF INFORMATION SECURITY

Data breaches can be costly. Major intrusions can tarnish a company's reputation, damage customer trust in electronic commerce, trigger lawsuits and send stock prices tumbling. Properly securing a service provider's databases which contain customers' personal information is critical for maintaining trust and preserving business continuity.

Securing and protecting personal information on a database makes good business sense. The expenses incurred through system down-time, reactively patching the system and upgrading the weakened infrastructure hit by a network intrusion could easily run into millions of euros. A recent study reported the costs associated with a major database intrusion could run to nearly €10 million.[5] The actual cost may be higher as many breaches are never reported to the public. As for the impact on a publicly held company's stock price, in the United States on average, news of a data breach immediately cuts about one percent off the traded value.[6] Stock valuations of some victims of a data breach dropped nearly 14% in the ensuing weeks as press coverage detailed a company's vulnerable data storage practices.

The EU member states also have a vested interest in the cyber security of databases storing traffic data. If this data is accessed by unauthorised parties, the confidence of EU citizens in the security of the information society in general, and the communication services to which the traffic data relates in particular, will be seriously shaken.

[5] Source: PGP Corp. study, 14 November 2005; www.pgp.com/news/ponemon_report.html.

[6] "Companies Pay a Price for Security Breaches", *Wall Street Journal*, 15 June 2005.

CONSIDERATIONS FOR POLICY

Data retention requirements in the draft Directive will require a considerable deployment of information technology and associated security measures. Observers estimate storage requirements will be 20,000 to 40,000 terabytes of data per year – the equivalent of 10 stacks of paper files each reaching from the earth to the moon.

Requiring an industry to store data is not new. Many industry sectors such as law firms, banks and accounting firms have developed regimes to hold data for seven years. However, currently there are very strict rules in place within the EU that regulate when and how personal information can be kept. The data protection directive, 95/46/EC, includes rules that stipulate that companies may only retain data necessary for the reason they are collecting the data and furthermore they have an obligation to destroy that data once it is no longer needed. The data retention directive could potentially roll-back some of these safeguards.

Traffic data in these repositories can significantly aid police and national security forces in their fight against terrorism and cyber crime. As the EU finalises legislation toward that goal, it must also ensure the use of a comprehensive database security protocol to protect personal information in the new databases.

CSIA urges EU legislators to include technologically neutral provisions which address data protection and data security in order to protect the data associated with EU citizens and maintain the free flow of data. Any data that is held in a database, no matter how long it is retained, should be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction or loss, alteration, unauthorised or unlawful disclosure or access, and against all other unlawful forms of processing. CSIA believes proper security of personal and traffic data is critical to maintaining citizen's trust in government and private institutions that retain such data. It is this trust that enables economic growth and stability.

About the Cyber Security Industry Alliance

The Cyber Security Industry Alliance is the only advocacy group dedicated to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education and awareness. The organization is led by CEOs from the world's top security providers, who offer the technical expertise, depth and focus to encourage a better understanding of security issues. It is the belief of the CSIA that a comprehensive approach to ensuring the security of information systems is fundamental to global protection and economic stability. Members of the CSIA include Application Security, Inc., BindView Corp.; Check Point Software Technologies Ltd.; Citadel Security Software Inc.; Citrix Systems, Inc.; Computer Associates International, Inc.; Entrust, Inc.; Internet Security Systems Inc.; iPass Inc. ; Juniper Networks, Inc.; McAfee, Inc.; PGP Corporation; Qualys, Inc.; RSA Security Inc.; Secure Computing Corporation, Surety, Inc.; Symantec Corporation; TechGuard Security, LLC, Visa International, and Vontu, Inc.

Cyber Security Industry Alliance

Europe

Bastion Tower
Marsveldplein/Place du Champ de Mars 5
B-1050 Brussels, Belgium
T 00 +32 2 504 7245

Global Headquarters

2020 North 14th Street
Suite 750
Arlington, Virginia 22201 USA
T 00 +1 703-894-CSIA
www.csialliance.org