DARKTRACE

DATA SHEET

Data Classification Policies - One Approach to Open Networks

Threat Background

One of the key realities about information security that organizations today have had to come to terms with is the fact that information ultimately cannot be secured simply by being kept within the corporate network.

In the past, it was common to rely on a simple binary separation between information that is within the company, and information that is outside. This has not been possible for some years and – from a security perspective – the situation continues to become more difficult. Modern organizations must contend with two serious problems in handling sensitive data.

The first is that networks today must necessarily be porous. It is crucial to the efficient functioning of an organization that certain kinds of information are able to flow freely in and out of its networks. Clients and customers often need important information to make good use of a product, for instance – information that may need to be kept confidential because it represents important intellectual property. Similarly, having access to a company's inventory data may be critical to achieving maximum production efficiency. Finally, independent consultants and other third parties are often given relatively unrestricted access to a company's internal network.

The second problem is that – for these reasons among others – we must accept that total network security is impossible. All networks will be subject to intrusion, by third parties as well as malicious insiders. Far from being something to be solved, this is a problem that has been getting worse for some time, and the trend is unlikely to be reversed in the foreseeable future. It is, unfortunately, a fact that organizations must learn to live with.

The ultimate conclusion that the existence of these two problems has forced organizations to reach is that the inside of the network cannot be treated as separate from the outside. Information circulating within the company is not all equally secure or insecure, nor is it equally important to keep all of it confidential. As a result, making distinctions between more and less sensitive data in this sense should be treated as a more important task than ever before.

Data Classification

One approach to this problem is to utilize a data classification policy. Many, if not most, modern organizations with a real concern for security utilize such a policy. The aim of a good data classification policy is to distinguish between different kinds of data with regard to confidentiality. Some of the data circulating within a given corporate network can be safely considered to be relatively undamaging even if widely publicized – simple conversations between employees about organizing tasks, marketing collateral, even financial details for small transactions. On the other hand, there is of course a great deal of data, from vital intellectual property to confidential deals with other organizations, that would be tremendously damaging to a company if released even to a few key third parties.

The purpose of a data classification policy is to ensure that data that has more potential to damage a company's competitive advantage or reputation if released will be kept safer than more quotidian information. If implemented well, such a policy allows companies to feel more confident that genuinely sensitive data, the release of which could seriously negatively impact the company itself or one of its clients or customers, is kept secure, while less sensitive data is able to move freely around the network or be sent outside the network where necessary.

Example Email Classification Policy

The primary means of communication in the vast majority of modern organizations remains email. A significant proportion of sensitive information passes through the company's email system at some point in its lifecycle, whether as an attachment or in the message text itself. As such, one of the most important aspects of a more general data classification policy is a policy for classifying email traffic. Such a policy should, today, be a core part of information security for companies dealing with sensitive data.

Level 0

- Encompasses the majority of email information produced or exchanged by employees and customers
- Covers operational and routine business dialogue
- Default server protection is required, but deliberate theft or accidental loss presents no prospect of material damage to the company or any of its customers

Level 1

- These are emails produced and exchanged by employees and customers containing details that, although not seriously damaging to the company or any of its customers, could negatively impact operations for one or both
- For example, the breach of one or more Level 1 emails could require expending time and capital to alter an established business process that can no longer be considered secure
- Level 1 therefore requires the sender to use certificate-based encryption on transmission

Level 2

- Infrequent communications containing sensitive operational or commercial material, the release of which has the potential to cause damage to the intellectual property, employee privacy, or commercial standing of the company or its customers
- Level 2 mail requires the highest level of certificate encryption available at server level on transmission or receipt

Level 3

- Infrequent emails with limited distribution containing the most sensitive commercial or customer information that is likely cause damage to intellectual property, employee privacy, or commercial standing of the company or its customers
- Level 3 requires the highest level of defense such as an additional encrypted container (with a password sent via a different non-TCP medium such as GSM or SMS), within the certificated mail and SSL tunnel provided by the server

About Darktrace

Named 'Technology Pioneer' by the World Economic Forum, Darktrace is one of the world's leading cyber threat defense companies. Its Enterprise Immune System technology detects previously unidentified threats in real time, powered by machine learning and mathematics developed at the University of Cambridge, which analyze the behavior of every device, user and network within an organization. Some of the world's largest corporations rely on Darktrace's self-learning appliance in sectors including energy and utilities, financial services, telecommunications, healthcare, manufacturing, retail and transportation. The company was founded in 2013 by leading machine learning specialists and government intelligence experts, and is headquartered in Cambridge, UK and San Francisco, including offices in Auckland, Boston, Chicago, Dallas, London, Los Angeles, Milan, Mumbai, New York, Paris, Seoul, Singapore, Sydney, Tokyo, Toronto and Washington D.C.

T: +44 (0) 1223 350 653 E: info@darktrace.com www.darktrace.com