Dell SecureWorks

Information Security Services

The value of threat intelligence

What problem does Counter Threat Unit Intelligence Services solve?

Having timely information on emerging threats and vulnerabilities allows an organisation to begin its protection, detection and mitigation responses more quickly. When conducting Threat Management, the speed of response is the critical factor in avoiding damage from emerging threats. Thus, the enterprise security professional must become aware of new threats and vulnerabilities in real-time as they emerge in order to perform their task effectively. As the number of vulnerabilities and threats increase exponentially, this task of information management and prioritisation becomes increasingly difficult for the information security team to manage internally. Threat intelligence allows an organisation to quickly prioritise and begin its remediation and threat prevention and protection efforts, without having to dedicate resources to tracking the flow of information through the security world.

How are organisations dealing with this problem today?

The standard way for the security professional to keep up with the deluge of events occurring in the security community is to subscribe to multiple mailing lists and to rely on vendor relationships. This results in an ever increasing number of emails, only a small fraction of which are relevant to their environment and the inability to attain necessary information during non-business hours. As the number of reported vulnerabilities continue to increase, with thousands more vulnerabilities being released each and every year since 2000 and the number of actual incidents increasing exponentially with regard to vulnerabilities, this solution becomes increasingly inefficient as time passes. As well, this solution is not a particularly good use of time, given the ineffectiveness of mailing lists as a source of information. Often, by the time a vulnerability or exploit has been reported on a mailing list, it has been known for a significant length of time by the security industry (either legitimate and/or illegitimate security experts). This ineffectiveness leads to companies that are relying on the traditional method being significantly behind the attacker in their ability to remain current with evolving threats.

Why should an organisation purchase Dell SecureWorks' Threat Intelligence service?

Dell SecureWorks' Counter Threat Unit (CTU) Intelligence Services provide a consistent, prioritised and customised way to track vulnerability and threat data that is relevant to the security professional and their environment 24X7. This eliminates the need to subscribe to an ever-increasing number of email lists or spend time attempting to build a network of vendor contacts to gather information. The Dell SecureWorks' research group is able to gather information not only through mailing lists, but through their extensive network of vendor relationships, formal and informal security contacts, and especially from the front lines of the security community. Dell SecureWorks' extensive global network of monitored devices enables the Dell SecureWorks' research group to gather information as it occurs in real-time, leading to zero-minute intelligence on newly emerging threats. This global visibility provides the enterprise with actionable real-world, real-time intelligence data. Dell SecureWorks' CTU Intelligence Services allow the security professional to apply their expertise to mitigating and managing risk, rather than reading email.

What are the benefits to the enterprise from CTU Intelligence?

The enterprise that has the Dell SecureWorks' CTU Intelligence Services benefit from an ability to more easily prioritise their remediation and threat mitigation efforts with high-quality, actionable, real-time data that is relevant to their environment. This enables the enterprise to better utilise their security team, as their security professionals are spending significantly less time attempting to separate signal from noise in all of the security list traffic and vendor announcements.

What is the benefit for the individual security professional who uses the service?

There are two benefits. The first is that the quality of information that Dell SecureWorks provides will be higher than the quality of information that is provided on the general security mailing-list; information gathered through Dell SecureWorks' global network of front-line devices and global network of both formal and informal relationships within the security community will be of significantly higher quality and credibility than information gathered simply by reading mailing lists (or by using services that simply collate mailing lists). In addition all information on a given vulnerability will be contained in a single location where the professional will be able to find information quickly and easily, rather than trying to collate from multiple sources.

What is it costing organisations not to have intelligence?

There are two scenarios for the customer that doesn't have Dell SecureWorks' CTU Intelligence Services. In the first, the customer has significant internal resources dedicated to keeping track of security mailing lists, either explicitly (i.e. someone is accountable for keeping up on security intelligence) or implicitly (i.e. security professionals within the organisation take it upon themselves to keep up on intelligence). In this case, it is easy to calculate the amount of time; if a full-time security professional is spending 50% of their time on reading mailing-lists (which is not uncommon), the math is simple. However, it is the case where nobody is keeping up on intelligence, or they are relying on a less real-world service to provide threat intelligence, the risk is more difficult to assess. How much does it cost the organisation to start patching their systems a full day later for the newest vulnerability? How much does it cost to learn about the new worm after 9 hours rather than in the first 10 minutes?

[1] CERT/CC Statistics 1998-2003: http://www.cert.org/stats/

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.