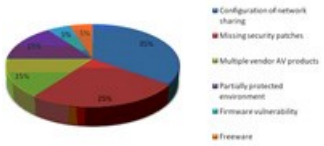
Why corporate networks are vulnerable

MOSCOW, RUSSIA: Kaspersky Lab, a leading developer of secure content and threat management solutions, presents the results of a study conducted by its Global Emergency Response Team - a consulting service for the company's corporate users. The data that was accumulated while serving corporate customers highlights the main IT security policy mistakes that can put an organisation at risk.

Commenting on the study, Alexey Polyakov, head of the Global Emergency Response Team at Kaspersky Lab, said: "In the past, our corporate support team received complaints unrelated to product functionality. For example, some customers complained that our products could not remove all the viruses from a network. After some quick analysis we discovered that the products did in fact successfully detect and remove malware, but this malware kept coming back - over and over again. So over the last 12 months, by actively engaging with our corporate users we have noticed that the majority of virus-related incidents occur due to underestimated design issues or unnoticed weaknesses in corporate security policies."

Why your corporate network may be vulnerable



click to enlarge

The biggest mistake is to ignore network share access rights - responsible for 35% of incidents. In such a case there might be open sharing with access rights configured as "full access" to everyone on an internal file server or end-user work desktop, e.g., a shared public document workspace where all documents are stored. Sooner or later this can become a prominent source of malware redistribution throughout the organisation.

Modern malware takes advantage of existing vulnerabilities. A network with just a single missing patch can be put at serious risk. And this is a common issue seen mostly in small to medium organisations with end-users numbering less than 500. These organisations either do not have enough expertise or ignore patching completely. As such, this mistake is responsible for 25% of incidents.

How security admin spends much of its time

Use of multiple vendor anti-malware solutions (15% of incidents) may lead to a situation where it is hard to mitigate malware attacks. This may occur if one of the vendors does not respond fast enough to attacks. Delays in responses may run to days, weeks or even months. During this time the solution of another vendor would detect and remove malware, but only in its part of the network - and malware would attack it from the unprotected side. Alexey Polyakov concluded, "From our experience we see that security admin spends a lot of time working with multiple vendors' support services in finding and fixing a problem."

A partially protected environment (15% of incidents) is where an anti-malware solution is installed on part of the network, leaving other resources unprotected.

Firmware vulnerability (5% of incidents) may be exploited by attackers if security admin forget to monitor hardware devices, such as routers, firewalls and other network appliances, to see if they need patching.

Also a mistake

In addition, another relatively infrequent mistake (also 5% of incidents) is to believe that software downloaded from the Web is always perfectly sound software.

Assistance on how to deal with these mistakes and what to keep in mind when designing a corporate IT security policy can be found in Alexey Polyakov's presentation entitled *Corporate Incidents: Lessons Learned. Common and Avoidable Security Policy Mistakes for IT Management* presented at the Kaspersky Lab International Technology Press Tour in Malaga, Spain. View the presentation at: http://www.kaspersky.com/international_technology_press_tour2011.

The Global Emergency Response Team (GERT)

GERT is a new consulting service for Kaspersky Lab's corporate users. The objective of the service is to help corporate customers identify and mitigate security policy mistakes and malware related outbreaks, perform forensic analysis, and provide security policy consulting. GERT is a globally distributed team. There are two major locations: Moscow, Russian Federation, and Seattle, USA.