Cyberattacks—attacks on computer systems—are a serious issue, making the headlines on an almost daily basis. The number of cyberattacks mounted by professional criminals, and even by nations, continues to increase, along with their sophistication and resultant severity, and this trend shows no sign of stopping.

According to a report from McAfee and the Center for Strategic and International Studies, cybercrime costs U.S. companies $100 billion annually—the equivalent of roughly $500,000 per employee—and adds up to a yearly global cost of over $500 billion.

Highly publicized incidents such as the 2013 Target data breach, where account details of 40 million of the retail chain’s customers were stolen, and the hacking and disclosure of confidential information belonging to Sony Pictures, as well as the recent U.S. government attack, where records containing personal information of over 20 million government employees were stolen from the Office of Personnel Management, have brought the problem to the forefront of public attention.

Even after a breach is known to have occurred, it is hard to maintain business continuity while implementing prompt countermeasures against possible further damage. The 2014 Heartbleed bug affected more than 100,000 servers around the world, and despite a patch being made available for this vulnerability within a week, three months later it was reported that 300,000 servers were still vulnerable, mainly due to a lack of efficient remediation tools.

The risks to corporate victims of cybercrime include reputational risk, resulting from loss of trust, and operational risk, where operations may be compromised or even suspended. An attack may involve the loss of confidential and proprietary information, which may lead to financial risk.

Perhaps worst of all, says Jun Goto, Senior Manager of NEC Corporation’s Cyber Security Strategy Division, many organizations have no idea that they have been attacked until the damage has been done.

Firewalls are not enough

With the proliferation of devices connected to the Internet, such as PCs, servers, network appliances and mobile devices, the “attack surface”—the number of possible points where cyberattacks can originate—continues to expand. With this increased attack surface comes increased complexity, and increased time needed to discover the points of unauthorized entry, and to issue appropriate software patches to correct the situation. Not only is more time needed, but a high level of technology and expertise needed to make it work are also required to implement an adequate degree of cybersecurity, and to mitigate attacks.

Even after rigorous measures are implemented, the most advanced security measures may still fail through over 30 percent of attacks, which may end up halting an enterprise’s operations. No wonder, says Goto, that cybersecurity is not simply the IT department’s problem; senior management will find that these issues affect them, as well.

NEC and partners look ahead

Being proactive is the order of the day. Rather than reacting catch-up and merely responding to threats from the bad guys, NEC takes a proactive approach, using intelligence from a variety of sources around the world to identify potential vulnerabilities in systems and applications, and threats to these systems. A primary information source is NEC partner Norse Corporation, a leading threat intelligence company that collects and analyzes 200 terabytes of cyberattack information daily.

As vulnerabilities are discovered, NEC’s professional security analysts determine which security patches should be distributed, and NEC’s solution pushes these and other threat intelligence items to system administrators, who are then deployed on a dashboard, and can then be applied.

Removing rotten apples from the barrel

As Goto points out, threat intelligence against its own is not enough to make a system secure. System administrators need to act on information in a speedy manner before hackers can do damage, and while some threats require the network to be isolated and restricted, others require immediate action. NEC’s solution is to be able to identify its traces and take appropriate countermeasures.

NEC’s Software-Defined Networking (SDN) solution, currently deployed in hundreds of installations, provides automated control of complex networks.

When malware is detected and a notice is sent, the administrator can press one button on a screen to isolate infected segments instantly, using the intelligence built into the SDN appliances.

NEC works with others to make a safer world

NEC’s skills and leadership in the field are recognized internationally. INTERPOL and NEC signed a partnership agreement, recognizing that both INTERPOL and NEC can draw on one another’s strengths to meet the digital crime challenges of today and tomorrow.

NEC continues to expand cybersecurity operations worldwide. Security Operations Centers have been established in Japan, Singapore, Australia and Brazil, providing peace of mind and security, and helping to protect safer cities and societies. NEC continues to develop and expand its fight against cybercrime. Additional security operations centers are planned for other countries to enable NEC to offer a full-service global service, no matter where in the world its customers may be operating.

[Learn more > http://www.nec.com/cybersecurity]