INFOTECH LEAD

eScan CEO on latest security trends and challenges for SMBs and enterprises

Recent spate of hacks and activism, coupled with industrial espionage, has forced enterprises to re-evaluate their security perspective and policies.

To counter the looming security threats, enterprise CIOs need to understand the functional aspects of day-to-day activities and habits of the users, said Govind Rammurthy, MD and CEO, eScan, to Infotech Lead.

It is important to devise Security Policies based on the business objectives and needs of the organization. They should make employees understand that security policies and security audits are as essential as monthly payroll processing and yearly accounting audit, according to Rammurthy.

Security audits/policies need not be within the comfort zone of each and every employee. eScan suggests that Centralized Management Console with remote deployment facilities will be much preferred.

eScan provides anti-virus and content security solutions for desktops and servers. The service is powered by technologies, such as MWL Technology, DIRC Technology, NILP Technol ogy, and sophisticated Anti – Virus Heuristic Algorithms.

The company recently launched eScan Total Security suite with Cloud Security for the SOHO segment, and is also preparing to launch eScan Security Solutions with Cloud Security for SMB and Corporates.

Recent spike in hacks and industrial espionage, which are forcing businesses to re-evaluate their security perspective and their security needs, has in a way contributed to the growth of the market. eScan is gaining popularity in Education, BFSI, Government, Telecommunication and Healthcare. These segments, Rammurthy says, are more open in adopting new technologies.

Usage and deployment of application firewalls, IPS, IDS, Mobile Security and endpoint device security are the recent security trends, for both the sections i.e. the enterprises and the hackers alike, Rammurthy said. While organizations are trying to protect/monitor these points of entry to ensure business continuity, the hackers/ APT actors are using these entry points to gain a foothold.

ROI for network security is purely based on the bandwidth cost at which information can be processed and a resolution be provided. Timely response is possible when using centralized dashboard for all networked devices will surely bring down the escalation timeline and will also assist in increasing the response time.

Latest trends such as Bring Your Own Device (BYOD), teleworking, urge for efficiency improvements, and growing compliance requirements are influencing security deployments in enterprises.

With the rapid expansion of external intelligent communication devices, which also doubles as storage devices, more and more organizations are finding it close to impossible to audit usage of mobile devices within corporate premises. Hence, there exists a very high possibility of data leakage, which leads to prioritizing security.

With many companies opting for 'work-from-home' strategies, with employees given their laptops and access to critical infrastructure using VPN's, once again usage of such access, usage of data (over the cloud) and tracking employee work schedules necessitates security.

Today, like in the West, as quality of manpower depletes, enterprises increasingly opt for relying on computing resources for ensuring efficiency of operations. Managing the ever increasing resources, and making best use of such resources, also leads to increased security awareness and implementation.

More and more countries now are bringing in mandatory compliance, regular audits and data backups for at least 5 years to ensure that in case of any lawsuits, companies can be forced to share information with regulatory authorities.

"Like, Income tax audits, sales audits, a time will come when governments will start asking enterprises for data-audits to check on the disciplinary aspects data sharing. Once again, security is a must for such audits," Rammurthy said.

Asset Management that affects the operational performance and business continuity is also one of the critical factors that should to be considered objectively while deploying security software. .

When asked about the price related concerns from CIOs, eScan CEO said the major concern of the CIOs is to ensure deploying new technologies, SLA compliance and business continuity while ensuring security of their IT infrastructure and controlling access to the corporate data in a cost-effective way.

Like big enterprises, SMBs need the same level of protection as enterprises in an easy to manage solution that is well tailored to fulfil the security needs of SMBs under constrained budgets, Rammurthy said. Some of the SMB verticals wherein IT is an integral part are education, government, hospitality and healthcare.

Elaborating on eScan's strategies in SMB segment, Rammurthy said, "SMB being one of the largest prospect segments for us, eScan has especially designed security solutions to fulfil the IT security needs of SMB segment. Moreover, being a channel centric brand, we have designed a special partner program that accelerates growth, offers marketing support and includes great sales incentives, all with increased profit for the geared SMB partners."

eScan now also facilitates Electronic Software Distribution (ESD) license keys to its partners. This helps them deliver eScan products to their customers 24×7 for any number of users, thus enhancing reach of eScan as well as margin for our channel partners.

IT is today an integral part of every business, SMBs are no exception. Adoption of technology platforms such as cloud, Smartphones, Tablets and high-speed Internet in SMBs has increased over the past few years. This growing IT reliance has led to IT security issues. Moreover, due to budget constraints, many SMBs do not have a dedicated and specialized team to take care of their IT infrastructure. This many a times leads to network downtime that affects business continuity, he added.

Rajani Baburajan