

Majalah PC, Malaysia (September 2008)

Headline: Bracing for Tough Times

Network security consolidation could hardly have arrived at a better time as IT professionals concerned with security are finding themselves at the center of a perfect storm caused by the convergence of three “threatening” conditions.

First, there’s the slowing growth of IT budgets. In a recent survey of IT decision makers by Computer Economics, the average expected growth in IT budgets was only 2.5 percent. And, since IT budgets depend to a large extent on company profits, the rough weather the economy is enduring can only further slow this growth rate.

Second is an unfortunate trend towards complacency about network security and compliance issues, if not among security professionals, then among the executive staff that controls the budget. In a sense, network security has become a victim of its own success in dealing with both new threats and new regulatory mandates like Sarbanes-Oxley. There has been no headline grabbing network-based attack for several years, and so many executives may feel that security has been “taken care of.” There is also a related tendency to concentrate on compliance issues at the expense of more traditional security issues, since their bottom-line impact is more readily discerned, and more in line with executive-level concerns.

Third, and perhaps most importantly, is the increasing complexity of network security: the growing sophistication of threats, an ever-increasing compliance burden, and vulnerabilities constantly exposed by new applications and technologies. Exploits are no longer so much focused on hacker reputation as on financial gain, and organized crime is moving in to take advantage of network security weaknesses. Of course, where there’s profit involved, innovation happens faster, so the scope and power of threats is changing more rapidly. The compliance burden is ever heavier as well, especially given the necessity of being able to prove that all possible steps were taken to protect sensitive data, which requires extensive logging and auditing. To top it all off, the very success of IT in supplying new applications to support business innovation and competitive advantage – not to mention popular applications like Skype and Facebook – has inevitably added new avenues of attack.

According to a market research firm Gartner, the most important way information security organizations will save money in 2008 is by leveraging the convergence of established security functions into network- or host-based security platforms that provide multiple layers of security in a single product to protect against an evolving multitude of network and content threats. In fact, Gartner estimates that, by 2010, only 10 percent of emerging security threats will require tactical point solutions, compared with 80 percent in 2005.

Furthermore, environmental consciousness is an issue customers are increasingly considering in the vendors they do business with. According to IDC, over 50% of customers take the “green” stance of a vendor into consideration when selecting a supplier, and one-third rate the availability of green offerings from an IT supplier as “important” or “very important.” This comes right from the top of the management chain as well: green IT is growing in importance for almost 80% of executives.

Consolidating your network security enhances security in three ways: better integration, more efficient management, and superior threat intelligence.

More Complete Threat Coverage

The threats confronting companies today are both network and content-based. Network threats include denial of service (distributed denial of service using “zombie” networks being particularly dangerous), eavesdropping and other intrusions and basic worms. These are dealt with using firewalls, Intrusion Prevention Systems (IPS) and VPNs. Content-based threats include more sophisticated worms, viruses, phishing and pharming, spyware, email spam and more, and require content-inspection technologies such as antivirus, antispam, web filtering and the like.

The rising sophistication of attackers, driven in part by the increasing involvement of organized crime, is also boosting the frequency of blended attacks that combine both network and content-level threats.

By enabling knowledge sharing between countermeasures, consolidating one's network security with a unified threat management (UTM) platform can greatly increase your ability to detect and prevent not only standard attacks but also more sophisticated multivector attacks. For instance, a consolidated system that couples a signature-based antivirus engine with a proactive intrusion prevention engine will be far more effective than a single-technique solution. Likewise, integrating web filtering, antivirus and IPS capabilities in a way that allows the various engines to correlate activity can greatly increase the ability to fend off sophisticated attacks. This correlation enables the system to initiate defense during the earliest possible phase of the attack, cutting down the likelihood of success and reducing related damage.

More Efficient Management

Consolidating network security via UTM can greatly improve the productivity of your security professionals by providing unified, centralized management of all the solution's capabilities, which of course is also necessary for scalability. This is an area where a non-consolidated approach is simply incapable of competing. There is certainly no practical way to unify and centralize management of a multi-vendor security solution. And even when a single vendor supplies a solution based on multiple boxes, even if it's called Unified Threat Management, the reality is that such vendors often assemble their offering from a collection of OEM solutions. This is especially likely to be true of vendors who are making the transition from a single-threat offering (e.g., Intrusion Prevention) to UTM. They build their UTM offering by adding OEM technologies to their core competency: antivirus from one vendor, intrusion prevention from another, and so forth. Such solutions are all too likely to offer a fragmented, partially-unified management approach whose complexity can compromise your ability to monitor and counter network and content-level threats.

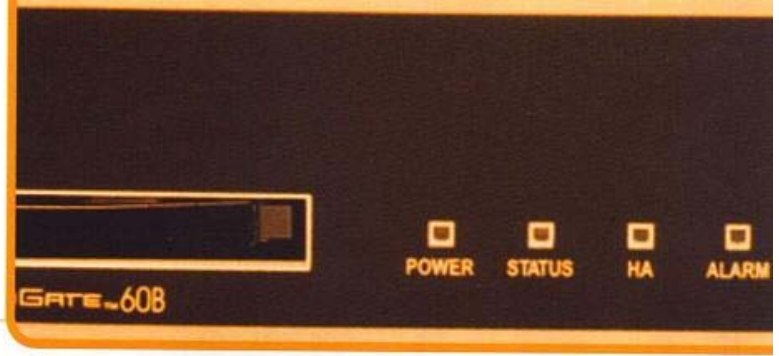
By contrast, many security management tasks become easier with a truly consolidated solution. Centralization gives you the ability to remotely manage multiple devices at once and supports other scalability features such as hierarchical policies and flexible grouping capabilities.

Superior Threat Intelligence

This is another area in which non-consolidated approaches often fall short, and for exactly the same reasons as discussed above under management. Vendors who rely on OEM technology to flesh out their offerings are dependent on the threat research offered by their suppliers. This makes it harder for you to judge the quality of the complete solution, and diffuses the responsibility for the research quality and timeliness. The existence of another link in the transmission chain from research lab to end-users can only make it more difficult to guarantee timely response, and hamper the responsiveness of the vendor's help desk. Because the understanding of various threats is diffused across multiple vendors, no matter how good their specialized knowledge is, the amount of cross-discipline knowledge-sharing is naturally limited, making it harder to understand multi-mode threats or how the various pieces of the solution can most effectively work together to counter them.

By contrast, the threat research behind a truly consolidated UTM solution will comprise an effort by a team of highly trained researchers experienced in a variety of threats and countermeasures, supported by knowledge-sharing structures and processes designed to highlight the ways in which multi-mode attacks can combine different threats. Likewise, team members charged with developing countermeasures will have a deep understanding of the synergies offered by the internal knowledge sharing of their UTM solution. This makes the detection of new threats, and the development of appropriate countermeasures, faster and more accurate. Such a threat research effort should also be global in nature, include automated feedback from the installed base of appliances as well as a manual means for customers to report new threats, and stress cooperation with major infrastructure vendors. This means that a large installed base is important; smaller vendors simply cannot offer the same degree of coverage.

This article has been contributed by Mr. Eryin Halmen, Country Manager of Malaysia & Brunei, Fortinet Inc.



Bersedia Untuk Masa Depan Yang Sukar



Penyatupaduan keselamatan rangkaian tiba pada masa yang amat sesuai kerana para profesional IT yang bimbang dengan keselamatan rangkaian kini mendapati bahawa diri mereka berada di pertengahan kemelut yang wujud akibat pertembungan tiga situasi.

FORTINET
REAL TIME NETWORK PROTECTION

Yang pertama, kemundaran bajet yang diperuntukkan untuk sektor IT. Baru-baru ini, tinjauan Computer Economics di kalangan para pengendali IT menunjukkan bahawa purata jangkaan pertumbuhan bajet IT adalah hanya pada 2.5 peratus. Oleh kerana bajet tersebut bergantung kepada keuntungan syarikat, keadaan ekonomi yang suram kini pasti akan terus memperlahankan kadar pertumbuhan bajet IT.

Situasi kedua, kewujudan sikap berpuas hati terhadap keselamatan dan isu-isu pelaksanaan keselamatan rangkaian. Trend malang ini wujud sama ada di kalangan profesional sekuriti atau golongan kakitangan eksekutif yang mengawal bajet syarikat. Dalam erti kata lain, keselamatan rangkaian telah menjadi mangsa kepada kejayaannya sendiri dalam pengendalian ancaman-ancaman baru serta mandat-mandat regulatori baru seperti Sarbanes-Oxley. Ketidakhadiran serangan besar sejak beberapa tahun yang lalu barangkali menyebabkan kebanyakan para eksekutif berpendapat bahawa isi keselamatan rangkaian telahpun diatasi. Terdapat juga kecenderungan syarikat untuk menumpukan perhatian mereka terhadap isu-isu pelaksanaan rangkaian tanpa mengambil kira isu-isu keselamatan tradisional kerana kesan keseluruhannya adalah lebih jelas dan lebih seiring dengan keinginan para eksekutif.

Faktor ketiga, iaitu faktor yang paling penting, adalah kerumitan keselamatan rangkaian yang semakin meningkat; pertumbuhan ancaman yang semakin canggih, bebanan pelaksanaan yang semakin berat dan kelemahan rangkaian yang semakin mudah terdedah dengan kewujudan aplikasi dan teknologi yang baru. Kini, eksploitasi tidak lagi tertumpu kepada peningkatan reputasi penggodam tetapi beralih kepada keuntungan. Operasi jenayah terancang kini juga mula mengambil kesempatan terhadap kelemahan-kelemahan dalam keselamatan rangkaian. Sememangnya, di mana terlibatnya keuntungan, inovasi baru akan dicipta dengan lebih cepat, sekaligus lingkungan dan kekuatan ancaman juga berubah dengan pesat. Bebanan terhadap pematuhan rangkaian juga semakin berat kerana

'logging' dan audit perlu dilakukan secara ekstensif agar dapat membuktikan kesemua langkah-langkah telah dilakukan untuk melindungi data-data yang sensitif. Selain itu, kejayaan IT dalam menyediakan aplikasi-aplikasi baru untuk menyokong inovasi perniagaan dan memberikan kelebihan untuk mengatasi pesaing-pesaing – serta kewujudan aplikasi-aplikasi popular seperti Skype dan Facebook – telah menyediakan ruang-ruang baru untuk diserang.

Mengikut firma penyelidikan pasaran, Gartner, kaedah yang paling penting bagi organisasi-organisasi keselamatan rangkaian untuk berjimat pada tahun 2008 adalah dengan menggalakkan penyatupaduan fungsi-fungsi keselamatan yang sedia ada kepada platform-platform keselamatan berdasarkan rangkaian atau hos. Ia memberikan keselamatan berbagai lapisan hanya dalam satu produk dan mampu melindungi rangkaian dari pelbagai ancaman dan ancaman konten yang semakin berkembang. Gartner juga menganggarkan bahawa hanya 10 peratus ancaman keselamatan bakal memerlukan penyelesaian pada tahap taktikal pada tahun 2010 berbanding dengan 80 peratus pada tahun 2005.

Selain itu, kesedaran terhadap penjagaan alam sekitar juga menjadi suatu kecenderungan bagi para pelanggan untuk bekerjasama dengan vendor. Menurut IDC, lebih dari 50 peratus pelanggan menitikberatkan pendirian sesebuah vendor dalam penjagaan alam sekitar apabila mereka membuat pilihan sebagai pembekal mereka. Satu pertiga daripada mereka juga meletakkan kepentingan yang tinggi terhadap keluaran produk-produk yang mampu menjaga alam sekitar. Golongan pengurusan atasan syarikat-syarikat juga mengambil berat mengenai dasar ini, di mana lebih kurang 80 peratus antara para eksekutif syarikat meletakkan kepentingan terhadap produk IT yang boleh menjaga alam sekitar.

Penyatupaduan keselamatan rangkaian meningkatkan keselamatan melalui tiga cara iaitu pengintegrasian yang lebih baik, pengurusan yang lebih cekap serta kecerdasan ancaman yang semakin hebat.



PERLINDUNGAN ANCAMAN YANG LEBIH LENGKAP

Ancaman-ancaman yang dihadapi oleh syarikat-syarikat hari ini terdiri daripada ancaman yang berdasarkan rangkaian dan ancaman konten. Ancaman rangkaian termasuklah penafian perkhidmatan (denial of service). Salah satu contoh ancaman yang paling berbahaya adalah penafian perkhidmatan menggunakan rangkaian "zombie", pemasangan telinga (eavesdropping) dan pelbagai lagi jenis pencerobohan dan juga worms asas. Ancaman ini boleh diatasi dengan penggunaan firewall, Intrusion Prevention Systems (IPS) dan VPN. Ancaman konten melibatkan worms dan virus-virus yang lebih canggih, phishing dan pharming, spyware, spam emel dan banyak lagi yang memerlukan teknologi pemensaan konten seperti antivirus, antispam, penapisan web dan selanjutnya.

Kecanggihan pengodam yang meningkat yang sedikit sebanyak disebabkan oleh operasi-operasi jenayah terancang yang semakin bertambah, telah mengakibatkan frekuensi serangan yang menggabungkan ancaman rangkaian dan konten melonjak naik.

Dengan membolehkan perkongsian maklumat tindak balas, menyatupadukan keselamatan rangkaian dengan platform pengurusan ancaman bersepadu (Unified Threat Management, UTM) dapat meningkatkan kebolehan anda untuk mengesan dan mencegah serangan-serangan yang biasa dan juga serangan multivektor yang lebih canggih. Sebagai contoh, sistem bersepadu yang menggabungkan enjin antivirus yang canggih dan enjin pencegahan pencerobohan yang proaktif adalah lebih berkesan daripada teknik penyelesaian yang tunggal. Pengintegrasian penapisan web, antivirus dan kebolehan IPS yang membolehkan aktiviti-aktiviti pelbagai enjin berhubungkait juga akan meningkatkan keupayaan untuk menangkis serangan-serangan yang canggih. Perhubungkaitan ini membolehkan sistem tersebut bersedia sedia untuk memberi perlindungan pada peringkat awal serangan, maka ia mengurangkan tahap kejayaan serangan itu sekaligus mengurangkan kerosakan yang mungkin terjadi.

PENGURUSAN YANG LEBIH CEKAP

Penyatupaduan keselamatan rangkaian secara UTM akan mempertingkatkan produktiviti golongan sekuriti profesional. Kebolehan sistem penyelesaian disatupadu dan diuruskan secara berpusat. Ini adalah satu bidang di mana pendekatan tanpa gabungan sememangnya tidak dapat bersaing. Tiada cara-cara yang praktikal untuk menyatupadu dan memusatkan pengurusan sistem penyelesaian sekuriti daripada pelbagai vendor. Meskipun suatu vendor membekalkan satu sistem penyelesaian berdasarkan pelbagai pakej dan menamakannya sebagai pengurusan ancaman bersepadu, realitinya, vendor tersebut seringkali mengumpul produk mereka daripada produk-produk pelbagai OEM. Ini adalah kenyataan terutamanya bagi vendor-vendor yang sedang mengalami transisi dari menawarkan sistem penyelesaian ancaman tunggal (contohnya pencegahan pencerobohan) ke UTM. Vendor-vendor tersebut membina sistem UTM mereka dengan menggabungkan pelbagai teknologi OEM dengan produk dasar mereka seperti perisian antivirus daripada satu vendor, perisian pencegahan penceroboh daripada vendor yang lain dan seterusnya. Barangkali,

sistem penyelesaian sebegini menawarkan satu sistem pengurusan yang berfragmen dan hanya separa bersepadu sekaligus wujudnya sebuah sistem yang amat rumit. Keadaan ini boleh menjejaskan kebolehan syarikat untuk mengawasi dan menentang segala ancaman rangkaian dan konten.

Jika dibanding, kebanyakan tugas pengurusan sekuriti menjadi lebih mudah dengan penggunaan sistem penyelesaian yang benar-benar bersepadu. Pemusatan memberikan anda keupayaan untuk menguruskan pelbagai peranti dari jauh secara serentak dan menyokong ciri-ciri pengukuran yang lain seperti polisi berhierarki dan kebolehan untuk pengumpulan yang fleksibel.

KECERDASAN ANCAMAN YANG HEBAT

Ini merupakan satu lagi bidang di mana sistem penyelesaian tidak bersepadu tidak dapat menandingi sistem penyelesaian pengurusan ancaman bersepadu atas sebab-sebab yang sama sepertimana yang dibincangkan dalam faktor-faktor pengurusan. Vendor-vendor yang bergantung kepada teknologi OEM untuk memadatkan produk tawaran mereka bergantung kepada penyelidikan ancaman yang dilakukan oleh pembekal mereka. Ini menyukarkan anda untuk mengetahui kualiti sebenar sebuah sistem penyelesaian yang lengkap, serta kualiti penyebaran penyelidikan dan ketepatan masa sistem tersebut. Kewujudan pautan yang lain dalam rangkaian transmisi dari makmal penyelidikan kepada pengguna akhir menyebabkan ia lebih sukar untuk menjamin respon yang cepat serta melembapkan kadar respons daripada bahagian bantuan vendor tersebut. Walaupun setiap vendor memahami dengan baik tentang bidang pengkhususan mereka, namun perkongsian maklumat antara mereka adalah terhad kerana penyebaran maklumat terlalu luas di serata vendor berbeza, maka adalah sukar untuk disatukan. Ini akan menyukarkan pengguna memahami pelbagai mod ancaman dan bagaimana sistem penyelesaian mereka dapat berkerjasama untuk menghalang ancaman-ancaman tersebut.

Penyelidikan ancaman oleh sistem UTM yang benar-benar bersepadu terdiri daripada usaha bersama sebuah kumpulan penyelidik berpengalaman dan terlatih serta dibantu dengan struktur dan proses perkongsian maklumat yang direka untuk menyelidik cara-cara serangan pelbagai mod boleh digabungkan dengan ancaman-ancaman lain. Ahli-ahli kumpulan yang ditugaskan untuk membangunkan kaedah-kaedah untuk menangkis serangan pula akan mempunyai kefahaman yang mendalam mengenai sinergi yang ditawarkan melalui perkongsian maklumat internal daripada sistem penyelesaian UTM itu. Dengan cara ini, ancaman-ancaman terberu dapat dikesan dan langkah penyelesaian dapat dilakukan dengan lebih cepat dan tepat. Cara penyelidikan ancaman seperti ini sepatutnya dilakukan secara global dan sebaiknya mendapat maklumbalas secara automatik daripada aplikasi-aplikasi asas. Ia juga seharusnya membolehkan para pelanggan melaporkan ancaman terbaru secara manual dan menekankan kerjasama antara vendor-vendor infrastruktur yang besar. Ini menunjukkan kepentingan pemasangan aplikasi dasar yang besar kerana vendor-vendor yang kecil tidak mampu memberi liputan yang sama luas.