CÔNG CỤ BẢO MẬT TẤT CẢ TRONG MỘT

Worm có thể lây lan qua spam và spyware có thể gieo mầm Trojan, hàng loạt mối đe dọa phức tạp mới sẽ không còn phân biệt rõ ràng nữa. Để ứng phó, cần có phần mềm bảo mật kết hợp nhiều công cụ khác nhau để giữ an toàn cho PC của bạn.Bạn có thể

Worm có thể lây lan qua spam và spyware có thể gieo mầm Trojan, hàng loạt mối đe dọa phức tạp mới sẽ không còn phân biệt rõ ràng nữa. Để ứng phó, cần có phần mềm bảo mật kết hợp nhiều công cụ khác nhau để giữ an toàn cho PC của bạn.Bạn có thể xây dựng hệ thống phòng thủ bằng các chương trình chống virus, chống spyware và firewall độc lập hoặc trang bị một ứng dụng tích hợp tất cả trong một. Chiến thuật sử dụng những ứng dụng bảo vệ chuyên biệt cho phép người dùng có được sản phẩm tốt nhất trong từng thể loại nhưng việc vận hành có thể phức tạp và chi phí đắt. Các sản phẩm tích hợp cung cấp sự tiện lợi và giá rẻ; các thành phần riêng lẻ của nó có thể được cấu hình cùng một giao diện và được thiết kế để có thể tương tác với nhau một cách trơn tru. Điều này có nghĩa là bạn phó thác hoàn toàn máy tính và dữ liệu của mình cho một công ty, nhưng còn hơn là gây rối loạn hệ thống với việc chạy nhiều phần mềm chống virus và firewall của nhiều hãng khác nhau.Cuộc chiến giữa các tên tuổi Để tìm được những bộ sản phẩm đáng giá, nhóm thử nghiệm (NTN) chọn 10 sản phẩm - bao gồm những sản phẩm mới và những sản phẩm đã có tên tuổi - để "tỷ thí" về hiệu suất và tính tiện lợi.

Symantec làm việc tốt, nhiều tính năng, dễ dùng.

Thử nghiệm xem xét 4 yếu tố: hiệu suất (phát hiện malware và tốc độ), tính năng, thiết kế (dễ dùng) và giá. Các sản phẩm có giá từ 40-80USD với 1 năm cập nhật miễn phí, phí các năm tiếp sau từ 25-60USD. Về hiệu suất, nên nhớ rằng phần mềm bảo mật chỉ tốt với cập nhật mới nhất (có thể là nhận dạng virus mới hay cải tiến phương thức quét virus). Về tính năng, nhìn chung các sản phẩm khá tương đồng.Để đánh giá phần thiết kế, NTN dựa trên tiêu chí cài đặt đơn giản và các tính năng dễ truy cập. Ngoài ra, NTN cũng đánh giá mức độ chi tiết của các cảnh báo và khả năng

huấn luyện chương trình. Điều quan trọng nhất là NTN chú ý vào hiệu suất, xác định khả năng phát hiện và cô lập những hiểm họa cũng như dọn sạch những chương trình độc hại. NTN kết hợp với công ty AV-Test.org để cho hơn 174.000 sâu, virus, cổng hậu, bot và spyware tấn công mỗi sản phẩm. Ngoài ra, AV-Test.org còn phân tích cơ chế thông minh (khả năng phát hiện những phần mềm độc hại chưa được nhận dạng). NTN sử dụng WorldBench 5 để đo hiệu suất của hệ thống khi thiết lập chế độ bảo vệ cao nhất.Tuy nhiên, NTN không đánh giá một cách đầy đủ khả năng phát hiện dựa trên hành vi. Công nghệ này (Microsoft, Panda, và Zone Alarm đều có cung cấp) có khả năng phát hiện những hiểm họa mới bằng cách "bắt" những hành động của các ứng dụng (ví dụ một chương trình muốn thay đổi registry). Tính năng này có thể bổ sung cho cơ chế nhận dạng, nhưng việc thử nghiệm nó đầy đủ không thích hợp với khuôn khổ bài đánh giá này. Các ứng dụng bảo vệ tốt nhất

Sản phẩm của Aluria quét file đóng gói nhưng không xử lý trình nén thực thi.

Trong tất cả các gói sản phẩm được thử nghiệm, một số ở mức khá và không chương trình nào đạt xuất sắc toàn diện. Gói sản phẩm của Symantec được đánh giá tốt nhất vì hoạt động ổn định qua tất cả các thử nghiệm. Nó đạt điểm firewall tuyệt đối và về nhì trong thử nghiệm virus, backdoor, bot và Trojan. Ngoài ra, nó còn cung cấp khả năng bảo vệ các ứng dụng IM (instant-messaging), công cụ quản lý truy cập Internet dành cho phụ huynh và tính năng bảo mật dữ liệu. Tuy nhiên, giao diện chương trình cần bố trí hợp lý hơn và chi phí hỗ trợ qua điện thoại "ngốn" tới 30USD mỗi lần.Về nhất ở khả năng chống malware trong đợt thử nghiệm này là gói sản phẩm McAfee, không chỉ thế sản phẩm này còn cung cấp những tính năng bổ sung khác như bảo vệ các ứng dụng IM, chống mạo danh (phishing) cho IE. Tuy nhiên, chương trình lại gây thất vọng ở tiến trình cài đặt và tốn tới 3USD cho mỗi phút hỗ trợ.Gói Zone Labs, tích hợp công cụ quét virus cũ của eTrust (của CA) xếp thứ 7 về hiệu suất, mặc dù là một firewall rất mạnh. Zone Labs có kế hoạch nâng cấp vào tháng 6. Dù sao, với nhiều tính năng và dễ dùng, gói sản phẩm này được xếp ở vị trí thứ 6 chung cuộc.Điều gây ngạc nghiên cho NTN chính là hiệu suất của BitDefender, tốc độ

chậm, quét adware bình thường, cộng thêm firewall kém ấn tượng, xếp thứ hạng 9.Tân binh Aluria có giá rẻ nhất nhưng các thành phần cơ bản lại xếp cuối. Phần mềm này có thể quét toàn bộ đĩa cứng nhưng không cho người dùng chọn tập tin và thư mục để quét. Ngoài ra, ứng dụng này không phát hiện được phần mềm độc hại khi được nén dạng thực thi như ASPack, UPX. Cuối cùng, thiết lập firewall mặc định của Aluria quá lỏng lẻo và "ngốn" nhiều tài nguyên hệ thống.

CHÚ THÍCH THUẬT NGỮ• Adware: phần mềm hiện quảng cáo và thu thập thông tin duyệt web của người dùng.• Backdoor: là một loại trojan nhưng nhiệm vụ chính là mở thông một số cổng nào đó trên máy tính để lây lan, truy cập và điều khiển máy tính từ xa.• Bot: loại chương trình chờ chỉ thị từ một nơi nhất định để thực hiện đồng loạt một hành vi nào đó. Bot là công cụ để thực hiện các cuộc tấn công DoS/DDoS.• Malware: phần mềm phá hoại.• Rootkit: một loại trojan nhưng tự giấu mình, hoạt động ở tầng thấp của hệ thống nên có thể ngăn cản một số dịch vụ. • Spam: thư rác.• Spyware: phần mềm dùng để theo dõi mọi hoạt động của máy tính và gửi về một địa chỉ nào đó.• Phishing: lừa người dùng Internet bằng cách tạo ra những trang web giả mạo để người dùng nhầm tưởng là web chính thức, dùng để lấy tài khoản ngân hàng, thẻ tín dụng, mật khẩu...• Trojan: phần mềm chỉ phát huy vai trò khi nhận một sự kiện nào đó.• Worm: sâu, lây lan qua thư điện tử hoặc lỗ hổng phần mềm.

Virus, spyware và adwareMcAfee và F-Secure đạt điểm số tốt khi phát hiện đâu là virus, đâu là spyware, điểm số của 2 sản phẩm này đều nằm trong "top 3". Sản phẩm Panda có cơ chế thông minh tốt nhất, McAfee và Aluria là 2 anh tài vượt trội trong phát hiện adware. Hầu hết các bộ sản phẩm đều phát hiện được 100% "tội phạm" trong WildList (danh sách công bố các virus, sâu và bot) tháng 1/2006. Aluria gây ngạc nhiên khi không phát hiện bất cứ boot-virus nào, sản phẩm của Microsoft không phát hiện 14 thành phần sâu, Trend Micro sót 2 thành phần sâu. Trong thử nghiệm với WildList, các thành phần boot-virus không đáng kể, điều này giải thích tại sao Aluria đạt điểm số 100% trong bảng đánh giá.

Panda bổ sung tính năng nhận dạng malware theo hành vi, tăng tính "thông minh".

Kết quả đối phó với 168.523 backdoor, bot và trojan của AV-Test rất khác nhau. CA chỉ phát hiện được 37% backdoor, 72% bot, 39% trojan. Zone Labs phát hiện 30% backdoor, 49% bot, và 31% trojan. F-Secure mạnh nhất, "tóm" hơn 98% các mối đe dọa.Trong thử nghiệm phát hiện adware, McAfee có điểm tốt nhất, "bắt gọn" 96% của 713 thành phần đang chạy. Aluria chiếm vị trí 2 với 89%. Một lần nữa Zone Labs có hiệu suất thấp, chỉ phát hiện 46% adware.Để đánh giá "trí thông minh", AV-Test.org kiểm tra khả năng "ứng xử" của các sản phẩm với các thành phần trong WildList mà không nhờ đến dữ liệu nhận dạng. Panda vượt lên với 91%, F-Secure về nhì nhờ "bắt" được 76%, Microsoft xếp cuối với 41% và Zone Labs xếp thứ hai từ dưới lên với 48%. Lưu ý, chức năng phát hiện dựa trên hành vi của những sản phẩm này có thể giúp cải thiện những điểm số kém cỏi trên. Thí dụ, AV-Test.org nhận thấy Panda TruPrevent có thể chặn tới 90% sâu mạng và email còn OS Firewall của Zone Labs chặn tới 70% sâu. NTN cũng đánh giá khả năng phát hiện phần mềm phá hoại (malware) gói trong tập tin nén như .zip, rar, .cab và các định dạng nén thực thi như ASPack và UPX. Đa phần các ứng viên có thể phát hiện ở mức nén một, nhiều lần hoặc dạng tự giải nén, nhưng lại thể hiện khả năng khác nhau ở định dạng nén thực thi. F-Secure, McAfee và BitDefender thực hiện tốt nhất, Aluria và Zone Labs xếp chót. Aluria cho biết phiên bản kế tiếp sẽ bổ sung khả năng "soi" file nén thực thi và được cập nhật miễn phí cho người dùng hiện tại vào cuối năm nay. Phía Zone Labs nói rằng họ đang làm việc với CA để cải thiện khả năng phát hiện malware "đóng gói" và OSFirewall sẽ phát hiện và cô lập ngay malware khi tập tin đóng gói được mở.Trong điều kiện lý tưởng, phần mềm bảo mật phải phát hiện và ngăn chặn tất cả các mối đe dọa từ dấu hiệu đầu tiên. Nhưng thực tế khó được như vậy. NTN kiểm tra khả năng quét sạch file, Registry và các file Host (tập tin khai báo các địa chỉ IP) bị lây nhiễm 10 sâu trong WildList. McAfee quét sạch phần mềm độc hại và khôi phục các thay đổi hệ thống, ngoại trừ một biến thể của Mytob nhắm vào chính các phần mềm bảo mật. Sản phẩm của Microsoft cũng làm khá tốt, làm sạch mọi loại sâu ngoại trừ các thay đổi trong Registry gây ra bởi Netsky.BA và Mytob.AR. F-Secure thể hiện khả năng tìm hơn là diệt, chỉ làm sạch được 5/10 sâu. Các firewall đối đầu

CA eTrust tích hợp firewall của Zone Labs

Ranh giới giữa phần mềm chống virus và phần mềm chống spyware đang mờ dần, nhưng các phần mềm firewall thì vẫn "tác chiến" độc lập, kiểm soát vào ra của mạng và cảnh báo hành vi đáng nghi.Firewall của 10 gói sản phẩm thử nghiệm đều cho phép thiết lập mức bảo mật tổng quát, danh sách ứng dụng an toàn và không an toàn, các cổng và giao thức được phép.Firewall tốt có thể phân biệt giữa tín hiệu tốt và xấu, thông báo tới người dùng những sự cố nghiêm trọng và cung cấp đủ chi tiết về hành vi được phát hiện, điều đó giúp người dùng quyết định có hay không nên để một ứng dụng nào đó hoạt động. Còn firewall kém thì thường xuyên đưa ra những thông báo mơ hồ và bạn có thể chặn nhầm ứng dụng mình cần hay tệ hơn là tắt cả firewall.Thử nghiệm các firewall dựa trên chế độ thiết lập mặc định để chặn các cuộc tấn công từ bên ngoài và phần mềm phá hoại có sẵn trên PC. Các sản phẩm của CA, Microsoft, Symantec và Zone Labs dập tắt hoàn toàn các đợt tấn công ngay bên trong, cụ thể: malware không thể vô hiệu firewall, xóa hay chiếm quyền hợp pháp (một vài malware sẽ ngụy trang thành IE và cố gắng thu thập các quyền mà bạn cấp cho IE) và backdoor không thể truy cập Internet.Với thiết lập mặc định, firewall của Aluria thất bại với tất cả cuộc tấn công từ bên trong, nhưng ở chế độ thiết lập cao nhất thì đều vượt qua cả 2 thử nghiệm chiếm quyền và backdoor. Aluria nói rằng chế độ mặc định mở cổng 80 và 443, nhằm mục đích giảm thiểu cảnh báo của firewall đến người dùng. Theo người phụ trách sản phẩm Aluria, hãng muốn để khách hàng tự cấu hình sản phẩm theo cách họ muốn.

Web Site Filter của Trend Micro có khả năng chặn web xấu

NTN cũng kiểm tra các firewall xem chúng có thể phát hiện những malware muốn đánh cắp dữ liệu của PC. Zone Labs đã giành được tròn 100 điểm, vượt 17 phép kiểm tra về chặn rò rỉ; Microsoft xếp thứ 2, vượt qua 7 thử nghiệm. Các sản phẩm khác đạt điểm rất thấp và Panda không vượt qua thử nghiệm nào hết. Lưu ý AV-Test.org chạy những tiện ích kiểm tra lỗ hổng đã được chuẩn hóa dành cho các nhà cung cấp sản phẩm bảo mật. Zone Labs phát triển sản phẩm để vượt qua các tiện ích kiểm tra lỗ hổng, trong khi đó Panda nói rằng chương trình không được tối ưu để chạy các ứng dụng kiểm tra, mà chỉ sử dụng công nghệ TruPrevent để phát hiện hành vi của những mã lệnh nguy hiểm.Trong thử nghiệm để đánh giá khả năng phản ứng với tấn công từ bên ngoài, các sản phẩm của CA, F-Secure, McAfee, Panda, Symantec và Zone Labs đạt 100%. Những sản phẩm này vô hiệu hoàn toàn các kiểu quét cổng thông dụng. Chúng chặn đứng các cố gắng truy cập vào PC thông qua cổng được mở để dùng cho việc chia sẻ file dựa trên giao thức SMB (Server Message Blocks), thông báo người dùng biết đó là truy cập an toàn hoặc truy cập có ý đồ xấu trong mạng máy tính gia đình. Chúng cũng không tiết lộ thông tin về HĐH của PC. Một lần nữa, firewall của Aluria thất bại 2/4 thử nghiệm ở thiết lập mặc định, tuy nhiên nó lại đạt 100% ở mức thiết lập cao nhất. Firewall của Trend Micro và BitDefender không khóa giao thức chia sẻ SMB và cả firewall của Microsoft cũng để lọt thông tin về HĐH.Nhiều hơn, nhiều hơn nữa

Các điều khiển của Zone Labs dùng cho trình IM khá mạnh

Tất cả các sản phẩm đều có khả năng chống spam, ngoài ra còn một số bổ sung khác nhau. Gói

sản phẩm của McAfee và Panda có nhiều tiện ích bổ sung nhất, ngược lại phần mềm của đại gia Microsoft lại có ít nhất (mặc dù OneCare tích hợp tiện ích sao lưu và kiểm tra đĩa).Ngoại trừ Aluria và Microsoft, tất cả sản phẩm còn lại đều muốn ghi điểm với các bậc cha mẹ, chúng cho phép người dùng khóa những thể loại website không lành mạnh, chẳng hạn: sex, cờ bạc, ma túy. Trend Micro cung cấp một tiện ích lọc URL tương đương, mặc dù không gọi tính năng này là "parental control" (tiện ích để cha mẹ có thể kiểm soát việc truy cập của trẻ nhỏ). Trong khi đó CA không cung cấp ngay trong sản phẩm của mình mà lại kèm CD riêng chứa K9 Web Protection của BlueCoat. Zone Labs sử dụng công nghệ Smart Filtering Dynamic Real Time để phân loại các website không nằm trong danh sách kiểm soát. BitDefender, McAfee và F-Secure gây bất ngờ hơn khi cho bố mẹ có thể xác định giờ giấc truy cập Internet.CA, McAfee, Symantec, Panda, Trend Micro đều cung cấp khả năng kiểm soát sự riêng tư để chống xâm nhập thông tin nhạy cảm như: thông tin thẻ tín dụng để lại trên máy tính, tuy nhiên chúng lại quá "thận trọng" ở mức thiết lập cao. Ví dụ, thiết lập mức an ninh cao nhất trong sản phẩm của Symantec sẽ luôn kích hoạt báo động khi một website yêu cầu nhận cookie trên hệ thống thử nghiệm, thậm chí đó là những website có tiếng tốt như của New York Times và pcworld.com, ở chế độ mặc định, các cookie loại này không được xem là có nguy cơ cao.Các tính năng thú vị khác: McAfee, Panda, Symantec và Zone Labs kiểm tra các ứng dụng IM để phát hiện đính kèm (Microsoft chỉ quét trên MSN Messenger). Panda, Trend Micro và Zone Labs cảnh báo người dùng có kết nối Wi-Fi bất hợp pháp (McAfee cũng đưa ra một sản phẩm bảo vệ kết nối Wi-Fi với giá 80USD).Một số tính năng bổ sung khá tiện lợi, nhưng một số khác lại chỉ làm rối giao diện. Điển hình như trình điều khiển tập trung của Symantec có một cửa sổ phụ để theo dõi các thành phần của bộ sản phẩm. Thêm một icon ở khay hệ thống thường xuyên hiện thông báo về tình trạng hoạt động. Nó còn tiếp thị cho các sản phẩm liên quan khác như phần Data Recovery hiển thị tình trạng thái "chưa có" cho đến khi bạn mua và cài đặt tiện ích SystemWorks giá 50USD.

HÃY ĐỂ ISP TRANG BỊ BỘ PHẦN MỀM BẢO MẬT Không ai vui vẻ gì khi bỏ tiền ra để mua các phần mềm bảo mật, nhưng người ta hiểu rằng chi phí đó là cần thiết để PC an toàn. Điều mà nhiều người không biết là họ có thể sử dụng các phần mềm đó miễn phí. Do hiểm nguy trên Internet ngày một gia tăng nên các nhà cung cấp dịch vụ Internet (ISP) lớn như AOL và Earthlink đều cung cấp những gói phần mềm bảo vệ cho khách hàng. Gói phần mềm chuẩn của AOLỨng dụng có tên Safety and Security Center bao gồm công cụ chống spam, công cụ kiểm soát truy cập Internet, chặn pop up và chống phishing của AOL được kết hợp với tường lửa, công cụ chống virus và spyware của McAfee. Gói phần mềm của AOL có dung lượng 28MB, gồm nhiều ứng dụng khác, nhưng đối với người dùng thì nó làm việc như là một ứng dụng thống nhất, xuyên suốt. Một trong những cách AOL hỗ trợ cho khách hàng là cô lập các đe dọa trên Internet ngay từ server, trước khi đến người dùng cuối. EARTHLINK chống spywareEARTHLINK cũng nỗ lực để tạo ra một ứng dụng bảo mật tất cả trong một và vì vậy họ đã mua Aluria - công ty phần mềm chống spyware - hồi năm rồi. Hiện tại, EARTHLINK cung cấp miễn phí gói phần mềm Protection Control Center cho khách hàng của mình và tính phí 5 USD/tháng cho người dùng khác. Phần mềm này có dung lượng 16MB, gồm các ứng dụng được tạo bởi 2 công ty và các ứng dụng chống virus và

tường lửa của đối tác Authentium.Tại sao các ISP gánh tất cả khó khăn và chi phí cho việc bảo mật? Đơn giản vì họ muốn làm cho khách hàng hài lòng .

Cài đặt và tiện ích

McAfee không phân biệt giữa adware và spyware mà gọi chung là PUP

Một sản phẩm được xem là dễ sử dụng khi việc cài đặt đơn giản, các tùy chọn cấu hình tổ chức tốt, chạy nhanh và thông báo rõ ràng. Microsoft và Trend Micro đáp ứng những tiêu chuẩn này rất tốt nhưng theo những cách khác nhau. Sản phẩm của Microsoft dễ cấu hình vì nó không có nhiều thứ để cấu hình! Điều này có thể làm cho người dùng cảm thấy hạn chế. Trong khi đó Trend Micro phân bổ rất tốt các tùy chọn trong giao diện đẹp và cấu trúc hợp lý.
Tất cả sản phẩm thử nghiệm đều cài đặt trơn tru và tự động cấu hình. Tuy nhiên, với sản phẩm của McAfee, cài đặt đầy đủ bộ phần mềm này người dùng phải khởi động lại máy 5 lần và tạo một tài khoản (tên người dùng/mật khẩu). Một hộp thoại đề nghị người dùng nhận thư thông tin về virus cũng như những thông tin khuyến mãi từ McAfee hoặc đối tác của McAfee. Ngoài ra, lúc đầu NTN không thể tải về phần cập nhật từ Firefox mà phải sử dụng IE và cho phép mở cửa sổ pop-up tạm thời.Sản phẩm của CA tích hợp kém nhất, đặt 4 biểu tượng ở khay hệ thống, cộng thêm giao diện chính không liên kết với các điều khiển của Blue Coat.Symantec có vẻ như "nhiều chuyện" nhất, thường xuyên cảnh báo về trạng thái và cookie. Nếu không thích, bạn có thể dùng sản phẩm của F-Secure vì nó có rất nhiều thiết lập chi tiết nhưng lại ít thông tin hướng dẫn.

Cảnh báo của Microsoft Firewall về hoạt động LimeWire trông ấn tượng hơn cu3a BitDefender.

Tốc độ quét của Panda nhanh nhất, mất khoảng 6 phút 39 giây với 14,7GB tập tin và thư mục trên hệ thống thử nghiệm. Trend Micro về nhì, 7 phút 37 giây. F-Secure chậm nhất, phải mất 28 phút 46 giây. F-Secure giải thích có tốc độ này là vì thực hiện bảo vệ theo thời gian thực và có tới 5 cơ chế quét gồm 2 cho virus, 1 cho spyware, rootkit và 1 quét thông minh.Trong kiểm tra sử dụng tài nguyên hệ thống, tất cả sản phẩm được cài đặt mặc định và đo trên WorldBench 5. Sản phẩm của Microsoft nạp nhẹ nhất, làm tăng thời gian thực hiện của 9 ứng dụng thử nghiệm lên khoảng 4% (mức "báo động" là 15%). Aluria ngốn nhiều tài nguyên nhất, tăng gấp đôi thời gian thực hiện của ACDSee PowerPack và Windows Media Encoder. BitDefender tiếp bước làm MS Office 2002 tăng 22% và Mozilla tăng 69%.Cảnh báo người dùng khi có dấu hiệu khả nghi, firewall của Microsoft cho thông tin chi tiết từ tên cho đến đường dẫn của những ứng dụng muốn truy cập Internet. BitDefender cấp thông tin về virus rõ ràng hơn ở firewall. McAfee đưa ra một khái niệm mập mờ, PUP (potentially unwanted program: chương trình không mong muốn tiềm ẩn), để phân loại adware hay spyware. Để có thông tin chi tiết về các thông báo của từng sản phẩm, bạn đọc có thể truy cập find.pcworld.com/53488.Nhìn chung, ngay cả những bộ sản phẩm được đánh giá cao của Symantec và McAfee đều không thực hiện hoàn thiện ở tất cả các nhiệm vụ. Với một số người "khó tính" và có kinh nghiệm, có thể họ vẫn muốn kết hợp và chọn lấy những thành phần tốt nhất từ các gói sản phẩm bảo mật. Nhưng với đa số người dùng thì tính tiện lợi của bộ phần mềm bảo mật trọn gói không gì sánh bằng.

10 THỦ THUẬT VẬN HÀNH BỘ PHẦN MỀM BẢO MẬTViệc cài đặt và chạy một bộ phần mềm bảo mật đầy đủ chức năng không đơn giản, nhất là bao gồm cả việc thay thế một sản phẩm của hãng này bằng sản phẩm của hãng khác. Dưới đây là các hướng dẫn cài đặt và bảo trì được tập hợp từ nhiều hãng bảo mật.1. Gỡ bỏ phần mềm chống virus cũ khỏi PC: Bạn chỉ nên chạy 1 lớp chống virus trên 1 máy tính. Gỡ bỏ hoàn toàn cái cũ, khởi động lại máy tính trước khi cài đặt cái khác. Ngoài ra, nên tắt tường lửa của Microsoft khi sử dụng tường lửa của một hãng khác, tuy nhiên một vài sản phẩm sẽ đề nghị bạn tắt tường lửa mặc định lúc cài đặt.2. Kiểm tra tình trạng "sức khỏe" đĩa cứng: tốt nhất nên chạy tiện ích Chkdsk của Windows vài lần trước khi tiến hành gỡ bỏ hay sửa c hữa các vấn đề với đĩa cứng của bạn. Nhấn start>run, gõ vào chkdsk, nhấn

OK.3. Cập nhật các bản vá Windows mới nhất: chạy ứng dụng cập nhật của Windows để đảm bảo hệ thống của bạn được cập nhật đầy đủ nhất trước khi cài đặt phần mềm bảo mật, cả những phần mềm bảo mật này người dùng cũng phải thường xuyên cập nhật. 4. Chuẩn bị thông tin: trong tình huống bạn gọi hỗ trợ từ hãng cung cấp, nên ghi ra giấy ngày cài đặt, số sản phẩm (serial number) và số điện thoại hỗ trợ. 5. Chạy một phần mềm chống spyware bổ sung: Nếu muốn bạn có thể chạy một tiện ích chống spyware riêng cùng với bộ phần mềm bảo mật, nhưng nên cẩn thận khi sắp lịch quét hệ thống và đảm bảo rằng chỉ một chương trình dò tìm cũng như cập nhật tại 1 thời điểm.6. Kết nối mạng: thường các máy tính nối mạng bằng VPN và có những thiết lập riêng. Nếu sau khi cài đặt bộ phần mềm bảo mật, máy tính bị treo khi khởi động lại, hãy ngắt kết nối mạng. Sau khi khởi động lại thành công, kết nối mạng trở lại và để bộ ứng dụng thiết lập cấu hình tường lửa cho bạn (đa phần các sản phẩm đều có wizard hướng dẫn).7. Xử lý vấn đề in ấn và chia sẻ file: tường lửa thường có cấu hình thiết lập sẵn để sử dụng dịch vụ chia sẻ tập tin và in trong mạng. Nếu không bạn phải tạo bằng tay để chỉ thị tường lửa cho lưu thông TCP ra cổng 1023 và vào cổng 139.8. Ghi lại những trường hợp khác lạ: nếu một sản phẩm xảy ra một sự cố đặc biệt - chẳng hạn một thông báo lỗi hay cảnh báo về ý đồ phá hoại – ghi lại chính xác toàn bộ thông điệp đó, thậm chí chụp cả màn hình.9. Gửi đi các file khả nghi: nếu gặp những tập tin hay e-mail đáng ngờ thì đừng mở nó và tự tìm hiểu nó. Hãy gửi chúng tới công ty cung cấp sản phẩm nhưng phải đảm bảo theo đúng qui trình. 10. Giữ quyền cập nhật: đây không phải là cường điệu vấn đề. Phần mềm bảo mật càng hiệu quả khi càng được cập nhật mới nhất và phần cập nhật bổ sung thường không cung cấp khi thời hạn đăng ký sử dụng của người dùng không còn giá trị. Khi một năm sử dụng đã hết đừng quên đăng ký tiếp hay thay thế phần mềm bảo mật khác.

Hải Phạm PC World Mỹ 7/2006