AN TOÀN THÔNG TIN - NÊN BẮT ĐẦU TỪ ĐÂU?

Khi nói đến an toàn thông tin (ATTT), điều đầu tiên người ta thường nghĩ đến là xây dựng tường lửa (Firewall) hoặc một cái gì đó tương tự để ngăn chặn các cuộc tấn công và xâm nhập bất hợp pháp. Cách tiếp cận như vậy không hoàn to&agrave

Khi nói đến an toàn thông tin (ATTT), điều đầu tiên người ta thường nghĩ đến là xây dựng tường lửa (Firewall) hoặc một cái gì đó tương tự để ngăn chặn các cuộc tấn công và xâm nhập bất hợp pháp. Cách tiếp cận như vậy không hoàn toàn đúng vì bản chất ATTT không đơn thuần chỉ là sử dụng một số công cụ hoặc một vài giải pháp nào đó mà để đảm bảo ATTT cho một hệ thống cần có một cái nhìn tổng quát và khoa học hơn. Vậy an toàn thông tin là gì? Không thể đảm bảo an toàn 100%, nhưng ta có thể giảm bớt các rủi ro không mong muốn dưới tác động từ mọi phía của các lĩnh vực hoạt động kinh tế xã hội . Khi các tổ chức, đơn vị tiến hành đánh giá những rủi ro và cân nhắc kỹ những biện pháp đối phó về ATTT, họ luôn luôn đi đến kết luận: những giải pháp công nghệ (kỹ thuật) đơn lẻ không thể cung cấp đủ sự an toàn. Những sản phẩm Anti-virus, Firewalls và các công cụ khác không thể cung cấp sự an toàn cần thiết cho hầu hết các tổ chức. ATTT là một mắt xích liên kết hai yếu tố: yếu tố công nghệ và yếu tố con người. 1. Yếu tố công nghệ: bao gồm những sản phẩm như Firewall, phần mềm phòng chống virus, giải pháp mật mã, sản phẩm mạng, hệ điều hành và những ứng dụng như: trình duyệt Internet và phần mềm nhận Email từ máy trạm. 2. Yếu tố con người: Là những người sử dụng máy tính, những người làm việc với thông tin và sử dụng máy tính trong công việc của mình. Hai yếu tố trên được liên kết lại thông qua các chính sách về ATTT. Theo ISO 17799, An Toàn Thông Tin là khả năng bảo vệ đối với môi trường thông tin kinh tế xã hội, đảm bảo cho việc hình thành, sử dụng và phát triển vì lợi ích của mọi công dân, mọi tổ chức và của quốc gia. Thông qua các chính sách về ATTT , lãnh đạo thể hiện ý chí và năng lực của mình trong việc quản lý hệ thống thông tin. ATTT được xây dựng trên nền tảng một hệ thống các chính sách, quy tắc, quy trình và các giải pháp kỹ thuật nhằm mục đích đảm bảo an toàn tài nguyên thông tin mà tổ chức đó sở hữu cũng như các tài nguyên thông tin của các đối tác, các khách hàng trong một môi trường thông tin toàn cầu. Như vậy , với vị trí quan trọng của mình , có thể khẳng định vấn đề ATTT phải bắt đầu từ các chính sách trong đó con người là mắt xích quan trọng nhất. Con người – khâu yếu nhất trong toàn bộ quá trình đảm bảo an toàn thông tin . Hầu như phần lớn các phương thức tấn công được hacker sử dụng là khai thác các điểm yếu của hệ thống thông tin và đa phần các điểm yếu đó rất tiếc lại do con người tạo ra. Việc nhận thức kém và không tuân thủ các chính sách về ATTT là nguyên nhân chính gây ra tình trạng trên. Đơn cử là vấn đề sử dụng mật khẩu đã được quy định rất rõ trong các chính sách về ATTT song việc tuân thủ các quy định lại không được thực hiện chặt chẽ. Việc đặt một mật khẩu kém chất lượng, không thay đổi mật khẩu định kỳ, quản lý mật khẩu lỏng lẻo là những khâu yếu nhất mà hacker có thể lợi dụng để xâm nhập và tấn công. Phương pháp đánh giá chất lượng hệ thống ATTT Có lẽ không một vị lãnh đạo nào dám khẳng định nội bộ công ty là thực sự an toàn và tin cậy. Trong bối cảnh nền kinh tế thị trường như hiện nay, sự canh tranh diễn ra gay gắt thậm chí giữa các nhân viên trong nội bộ công ty: tranh dành khách hàng , mục đích thăng tiến hoặc các mục đích không lành mạnh khác. Ở một số tổ chức, lợi dụng sự lỏng lẻo trong quản lý về ATTT, nhân viên đã có những hành vi bất lương như lấy cắp thông tin mật, chiếm đoạt tài khoản khách hàng , ăn cắp tiền thông qua hệ thống tín dụng… Theo thống kê, khoảng 70% các rủi ro về ATTT là xuất phát từ nội bộ trong tổ chức. Một trong những câu hỏi luôn được đặt ra trước các nhà lãnh đạo và các nhà quản trị thông tin là: “Hệ thống thông tin của tổ chức an toàn đến mức độ nào?”

Câu hỏi này là mối quan tâm lớn nhất và cũng là vấn đề nhạy cảm nhất trong các khâu quản lý hệ thống thông tin. Trả lời câu hỏi này thật không đơn giản nhưng không phải là không có câu trả lời. Để giải đáp vấn đề trên, chủ yếu dựa vào hai phương pháp đánh giá ATTT như sau: + Phương pháp đánh giá theo chất lượng ATTT của hệ thống bằng cách cho điểm.Ví dụ: hệ thống đạt 60/100 điểm hoặc 60% + Phương pháp đánh giá theo số lượng thiết bị - công nghệ bảo mật. Trong thực tế, phương pháp đánh giá theo chất lượng là phương pháp duy nhất để đánh giá mức độ an toàn của các tài nguyên trong hệ thống thông tin. Ở Việt Nam, việc đánh giá ATTT theo chất lượng là hoàn toàn mới. Người ta dễ ngộ nhận việc trang bị một công cụ ATTT như (Firewall, Anti-virus…) là đảm bảo được ATTT cho hệ thống. Chất lượng ATTT phải được đánh giá trên toàn bộ các yếu tố đảm bảo tính an toàn cho hệ thống từ tổ chức, con người, an ninh vật lý, quản lý tài nguyên … đến việc sử dụng các công cụ kỹ thuật. Nói cách khác, chất lượng ATTT được đánh giá trên cơ sở thực thi các chính sách về ATTT trong hệ thống. Các chính sách này được chuẩn hoá và được công nhận là các tiêu chuẩn về ATTT áp dụng trên phạm vi toàn thế giới. Phương pháp đánh giá theo số lượng không được sử dụng. Tiêu chuẩn đánh giá về chất lượng ATTT. Việc đánh giá mức độ ATTT của các tổ chức thường được tiến hành theo kinh nghiệm và dựa trên các quy định mang tính cảm tính , cục bộ của tổ chức đó mà không tính đến các tiêu chuẩn đã được thế giới công nhận . Vài năm trước đây, Viện Tiêu chuẩn của Anh (BSI) cùng với một số tổ chức thương mại khác như Shell, National Westminster Bank, Midland Bank… đã nghiên cứu và đề xuất một tiêu chuẩn về ATTT. Đến năm 1995, tiêu chuẩn này được công nhận là tiêu chuẩn quốc gia về quản lý ATTT - BS7799. Tiêu chuẩn này độc lập với mô hình hoạt động của các công ty. Lãnh đạo công ty, các CSO/CIO… đã dựa trên cơ sở các tiêu chuẩn này để thiết lập các chính sách ATTT cho đơn vị mình. Ngay sau khi ra đời, BS7799 đã được sử dụng ở 27 nước bao gồm các nước thuộc khối liên hiệp Anh cũng như một số quốc gia khác như Thụy Sỹ, Hà Lan... Đến năm 2000, Tổ chức tiêu chuẩn thế giới ISO trên cơ sở BS7799 đã xây dựng tiêu chuẩn ISO 17799 và tiêu chuẩn này trở thành tiêu chuẩn quốc tế về quản lý chất lượng ATTT (ISO/IEC 17799). Tính đến tháng 2/2005 đã có khoảng hơn 1000 tổ chức đã nhận chứng chỉ ISO 17799 trong đó có Hitachi, Nokia, Fujitsu, Siemen và rất nhiều hãng tên tuổi khác. Những phần cơ bản của ISO 17799: 1. Chính sách chung 2. An ninh nhân sự (Personel Security) 3. Xác định, phân cấp và quản lý tài nguyên (Asset Identification, Classification & Control). 4. An ninh vật lý (Physical Security). 5. An ninh tổ chức (Security Organization). 6. Quản trị IT và mạng (IT operations and network management). 7. Quản lý truy cập và các phương pháp (Access control & methods). 8. Phát triển HT và bảo trì (System development & maintenance). 9. Tính liên tục trong kinh doanh và kế hoạch phục hồi sau sự cố (Bussiness Continuty & Disaster Recovery Planning) 10. Phù hợp hệ thống với các yếu tố về luật pháp, đạo đức (Low, Inestigation and Ethics). Chính sách về an toàn thông tin được tổ chức theo mô hình kim tự tháp.Cách tổ chức này giúp cho các nhà lãnh đạo quản lý chất lượng an toàn thông tin một cách khoa học và hiệu quả. Trên đỉnh kim tự tháp mô tả các chính sách được áp dụng trong tổ chức .Tại sao ta phải thiết lập chính sách này ? Phạm vi và đối tượng tác động của chính sách? Không có một chính sách áp dụng chung cho mọi đơn vị. Trong một tổ chức có nhiều bộ phận , từng bộ phận lại có chức năng nhiệm vụ khác nhau, tính chất và cách tổ chức thông tin cũng khác nhau .Bộ phận kinh doanh có mô hình thiết kế hệ thống riêng với cơ sở dữ liệu mang đặc thù kinh doanh , bộ phận sản xuất ,bộ phận nghiên cứu cũng có cấu trúc hệ thống và cơ sở dữ liệu của riêng mình .Trình độ nhận thức về an toàn thông tin cũng rất chênh lệch . Chính vì vậy khi thiết lập các chính sách ,nhà quản lý cần xác định rõ mục đích của chính sách được thiết lập , đối tượng thực thi , phạm vi tác động… Lớp thứ hai trên mô hình mô tả

các quy tắc, quy định thực thi các chính sách. Để thực hiện các chính sách ta phải làm gì ? Hệ thống các quy tắc ATTT được thể hiện trên 10 lĩnh vực lớn bao hàm các quy định từ tổ chức, con người, an ninh vật lý đến các công cụ kỹ thuật an toàn thông tin. Các quy tắc được xây dựng trên mô hình IT chuẩn của tổ chức và thể hiện được tính đặc thù của tổ chức đó.Thông qua việc thực thi các quy tắc, có thể đánh giá chất lượng an toàn thông tin của một tổ chức thông qua kiểm toán (Audit) . Lớp thứ ba là lớp cuối cùng của mô hình . Đây là các quy trình , các giải pháp hỗ trợ thực thi các quy tắc , quy định trên.Nó trả lời cho câu hỏi làm như thế nào để thực thi các quy định trên ? Các nhà quản trị an toàn thông tin (CSO) cùng các quản trị IT thiết lập các quy trình này và phổ biến đến mọi nhân viên trong tổ chức ,ví dụ "Quy trình thay đổi mật khẩu","Quy trình cài đặt các chương trình diệt virut ,chống các chương trình độc hại " v.v.Các quy trình này có thể liên quan đến nhiều chính sách và đối tượng sử dụng khác nhau. Việc áp dụng ISO 17799 đem lại lợi ích gì cho tổ chức? Việc áp dụng các tiêu chuẩn về ATTT theo ISO 17799 làm tăng nhận thức cho đội ngũ cán bộ nhân viên về ATTT. Xây dựng một môi trường an toàn, có khả năng miễn dịch trước các rủi ro, giảm thiểu các nguy cơ do con người gây ra. Tiêu chuẩn ISO 17799 đề ra những nguyên tắc chung trong quá trình thiết kế , xây dựng hệ thống thông tin một cách khoa học, giúp cho việc quản lý hệ thống trở nên sáng sủa, an toàn, minh bạch hơn. Chúng ta xây dựng một "bức tường người an toàn" (Secure People Wall) trong tổ chức. Một môi trường thông tin an toàn, trong sạch sẽ có tác động không nhỏ đến việc giảm thiểu chi phí vật chất đầu tư cho ATTT vốn dĩ rất tốn kém. Về lâu dài, việc nhận được chứng chỉ ISO 17799 là một lời khẳng định thuyết phục với các đối tác, các khách hàng về một môi trường thông tin an toàn và trong sạch . Tạo điều kiện thuận lợi cho sự hội nhập một môi trường thông tin lành mạnh. Điều này sẽ tác động mạnh đến ưu thế cạnh tranh của tổ chức. Vấn đề đào tạo nguồn nhân lực Theo IDG vào khoảng năm 2006 sẽ bùng nổ một nghề mới trong lĩnh vực IT – nghề an toàn thông tin.Chức danh CSO (Chief Security Officer) trở nên quen thuộc trong lĩnh vực IT. Cập nhật và nâng cao kiến thức về ATTT và nhận thức về vai trò của nó trong hệ thống IT là một điều rất quan trọng và cấp bách vì xét cho cùng hành động của con người là yếu tố quyết định . Mặc dù ATTT được biết đến rộng rãi nhưng yếu tố con người thường ít được các tổ chức quan tâm đến. Đối với những nhà quản trị, họ cần một chính sách an toàn và một chương trình nhận thức cũng như đánh giá chất lượng về ATTT nhưng tiếc rằng hiện nay chưa có nhiều giải pháp thực sự quan tâm vào vấn đề làm sao để tăng cường sự vững chắc cho mối liên kết vốn dĩ rất yếu ớt này trong mắt xích ATTT. Hiện nay, một số doanh nghiệp tại Việt Nam đã có sự chuyển biến tích cực trong vấn đề nhận thức về ATTT. Họ sẵn sàng đầu tư ngân sách đào tạo nguồn nhân lực nhằm tạo nền tảng vững chắc về nhận thức và kiến thức ATTT cho đội ngũ nhân viên của doanh nghiệp. Điển hình là như: Sở Khoa học và Công nghệ Đồng Nai, Công ty Bảo hiểm Bảo Minh, Fujitsu Vietnam, Ngân hàng Á Châu ... Bên cạnh đó vẫn còn nhiều doanh nghiệp nhất là các doanh nghiệp vừa và nhỏ vẫn chưa tiếp cận và hiểu hết tầm quan trọng của việc thiết lập các chính sách về ATTT và quản lý tiêu chuẩn chất lượng ATTT theo ISO 17799 thực sự vẫn còn xa lạ và mới mẻ đối với họ. An toàn thông tin nói chung và đánh giá chất lượng về an toàn thông tin nói riêng vẫn còn là vấn đề mới ở Việt Nam .Hy vọng bài viết giúp cho các nhà quản lý , các nhà hoạch định chính sách có thêm thông tin về vấn đề quản lý chất lượng ATTT cũng như cách tiếp cận với vấn đề an toàn thông tin – một vấn đề hết sức nhạy cảm hiện nay.Đồng thời bài viết cũng nêu rõ vai trò của con người – khâu yếu nhất trong đảm bảo an toàn thông tin cũng như tầm quan trọng của vấn đề đào tạo nguồn nhân lực trong lĩnh vực này T.S Đào Thế Long - Misoft ISTC Email: tan.document@gmail.com