CHUYỂN BIẾN NHẬN THỨC VỀ AN NINH MẠNG TRONG ĐẠI DỊCH COVID-19 CỦA CÁC DOANH NGHIỆP VỪA VÀ NHỎ

HOÀNG YẾN

Ứng dụng kỹ thuật số càng nhiều thì bình diện để tin tặc tấn công càng rộng. Nhưng trong một thế giới số, việc liên tục gia tăng các ứng dụng kỹ thuật số là không thể tránh khỏi. Điều này khiến công tác đảm bảo an ninh mạng trở nên vô cùng khó khăn, đặc biệt với các doanh nghiệp vừa và nhỏ (Small and Medium sized Businesses - SMB), có nguồn tài chính và nhân lực eo hẹp. Do đó, việc đầu tư đảm bảo an toàn an ninh thông tin đối với các SMB cần được tính toán kỹ lưỡng và theo trình tự khoa học. Nhưng điều quan trọng nhất và cũng là bước đi đầu tiên để xác lập hệ thống an ninh mạng là cần phải đánh giá chính xác điểm mạnh, yếu trong hệ thống thông tin của mình cũng như những rủi ro tiềm ẩn có thể xảy ra. Từ đó, các SMB mới có cơ sở vững chắc để xây dựng thế trận an ninh mạng phù hợp nhất với đơn vị mình.

Gia tăng rủi ro từ ưu tiên kỹ thuật số

Đại dịch COVID-19 đã thúc đẩy nhu cầu đầu tư vào các giải pháp và năng lực công nghệ giữa các tổ chức thuộc mọi quy mô. Khi bắt đầu đại dịch, các doanh nghiệp đã chuyển sang sử dụng công nghệ để tồn tại. Mục đích là hoạt động và tiếp tục phục vụ khách hàng ngay cả khi toàn bộ nền kinh tế rơi vào tình trạng ách tắc và phần lớn lực lượng lao động đã chuyển sang bố trí làm việc từ xa. Chúng ta đã chứng kiến tác động tích cực mà công nghệ có thể mang lại, và với việc các quốc gia hiện đang dần dần mở cửa lại nền kinh tế, tất cả các tổ chức đều mong muốn tận dụng nó để phát triển mạnh trong trạng thái bình thường mới. Điều này đặc biệt đúng đối với các doanh nghiệp vừa và nhỏ (SMB) trên khắp châu Á Thái Bình Dương. Nghiên cứu "An ninh mạng dành cho SMB: Các doanh nghiệp châu Á Thái Bình Dương chuẩn bị cho Phòng vệ kỹ thuật số" của Cisco có góc nhìn toàn cảnh về xu hướng công nghệ, đặc biệt là liên quan đến an ninh mạng của các SMB.

Nghiên cứu cho thấy 94% SMB trong khu vực đã áp dụng một số hình thức công nghệ. Đáng khích lệ hơn nữa là đại đa số (90%) đều có lộ trình số hóa. Điều này được nhấn mạnh ở Thái Lan, nơi 99% SMB có lộ trình và ở Ấn Độ, nơi 95% SMB có lộ trình. Tuy nhiên, con số này thấp hơn một chút ở các nền kinh tế trưởng thành như Nhật Bản và Hàn Quốc, nơi lần lượt 77% và 75% SMB cho biết họ có chiến lược hoặc lộ trình số hóa.

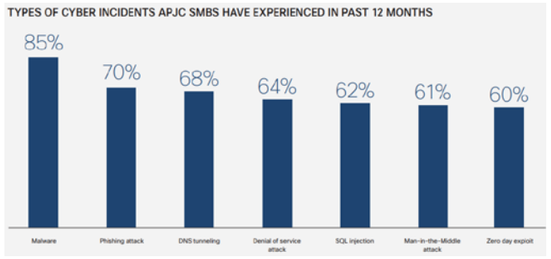
Khi nói đến việc triển khai, 65% SMB đang thực hiện tốt hành trình số hóa của họ, đã triển khai hơn 50% kế hoạch số hóa cho đơn vị mình. Các SMB ở Indonesia, Ấn Độ và Đặc khu hành chính Hồng Kông đã đi được ít nhất nửa chặng đường. Đặc biệt, Đài Loan, Malaysia và Hàn Quốc là những nước đi xa nhất.

Khi quá trình số hóa giữa các SMB trong khu vực đang tăng tốc, ngày càng có nhiều sự tập trung vào an ninh mạng, đặc biệt là do sự gia tăng bề mặt tấn công mà tin tặc và các tác nhân độc hại khai thác, phản ánh tốc độ số hóa. Không có gì ngạc nhiên khi 3/4 số SMB cho biết ngày nay họ quan tâm hơn đến vấn đề an ninh mạng so với 12 tháng trước. Con số này là rất đáng kể và cũng đáng khích lệ vì nó cho thấy mức độ nhận thức về rủi ro mạng của các SMB được nâng cao.

Những lo sợ đối với mất an toàn thông tin là có cơ sở. Nghiên cứu của Cisco cho thấy hơn một nửa (56%) các SMB ở châu Á Thái Bình Dương đã trải qua một sự cố mạng trong năm qua với nhiều nạn nhân của tội phạm mạng. 85% các tổ chức, doanh nghiệp bị tấn công bằng phần mềm độc hại. Kết quả của những sự cố này là những kẻ xấu đang lấy được dữ liệu có giá trị, từ thông tin khách hàng (75%), email nội bộ (62%), dữ liệu nhân viên (61%) đến tài sản trí tuệ (61%) và chi tiết tài chính (61%).

Trong số những người bị sự cố mạng, một phần ba (33%) được xếp hạng là không có giải pháp an ninh mạng là lý do hàng đầu. Mặc dù vậy, một số lượng lớn hơn các SMB (39%) cho biết yếu tố số một là các giải pháp an ninh mạng của họ không đủ để phát hiện và ngăn chặn một cuộc tấn công. Điều này cho thấy thực tế rằng, việc có công nghệ phù hợp là rất quan trọng để xây dựng một thế trận an ninh vững chắc. Trong số các tổ chức, doanh nghiệp đã trải qua sự cố, họ đã nhìn thấy vô số cách khác nhau mà những kẻ tấn công cố gắng xâm nhập vào hệ thống của mình. Các cuộc tấn công bằng phần mềm độc hại, ảnh hưởng đến 85% các SMB, dẫn đầu bảng xếp hạng. Việc tăng cường áp dụng và sử dụng các thiết bị như máy tính xách tay, máy tính bảng và điện thoại thông minh đã chứng kiến những kẻ tấn công ngày càng cố gắng triển khai phần mềm độc hại trên các thiết bị cầm tay này.

Các SMB đang bị nhắm mục tiêu bởi những kẻ tấn công tìm cách triển khai phần mềm độc hại với mục đích làm gián đoạn, làm hỏng hoặc truy cập trái phép vào các thiết bị đang được nhắm mục tiêu. Sự quan tâm của những kẻ tấn công đối với các SMB có thể do một số khía cạnh chính. Thứ nhất, trong cộng đồng hacker có quan niệm rằng các SMB tương đối yếu hơn trên mặt trận an ninh mạng so với các tổ chức lớn khiến họ trở thành mục tiêu hấp dẫn. Thứ hai, các SMB đang ngày càng làm việc nhiều hơn với các tập đoàn lớn dưới hình thức này hay hình thức khác. Các tin tặc hy vọng là nếu họ có thể xâm nhập vào mạng của một SMB cụ thể, họ có thể sử dụng mạng đó làm bệ phóng để sau đó truy cập vào mạng của một tập đoàn lớn hơn mà SMB này có thể đang làm việc hoặc thực hiện các giao dịch hoặc liên lạc kỹ thuật số.



Các loại tấn công mạng chủ yếu nhằm vào các SMB khu vực châu Á Thái Bình Dương trong 12 tháng qua.

Theo những người được hỏi, các cuộc tấn công bằng phần mềm độc hại sau đó là lừa đảo, với 70% nói rằng họ đã trải qua các cuộc tấn công như vậy. Các hình thức tấn công hàng đầu khác mà người trả lời báo cáo bao gồm: mã hóa dữ liệu của các chương trình hoặc giao thức khác trong các truy vấn DNS và phản hồi (DNS Tunneling) chiếm 68%; từ chối dịch vụ DDOS (64%); tấn công các ứng dụng hướng dữ liệu, trong đó các câu lệnh SQL độc hại được chèn vào một trường nhập để thực thi (SQL Injection) là 62%; tự định vị trong cuộc trò chuyện giữa người dùng và ứng dụng khiến nó có vẻ như đang diễn ra một cuộc trao đổi thông tin bình thường với mục tiêu đánh cắp thông tin cá nhân (Man-in-the-Middle) là 61% và tấn công Zero Day chiếm 60% .

Điều này đang có tác động rõ ràng đến các SMB với 62% số người được hỏi nói rằng một sự cố mạng đã làm gián đoạn hoạt động của họ và 61% cho rằng nó dẫn đến mất doanh thu. Ngoài ra, 57% cho rằng mất lòng tin với khách hàng, trong khi 66% cho rằng sự cố mạng đã ảnh hưởng tiêu cực đến danh tiếng của công ty. Mặc dù không thể chứng minh được bằng những con số cụ thể, nhưng sự suy giảm danh tiếng và xói mòn lòng tin có thể gây ra những hậu quả tai hại cho bất kỳ doanh nghiệp nào.

Các doanh nghiệp Việt Nam đã nhận thức tốt hơn về an ninh mạng

Về mặt tích cực, các SMB nhận rõ được thách thức về an ninh mạng. Trên thực tế, tổ chức, doanh nghiệp đang thực hiện một cách tiếp cận có kế hoạch hơn để chiến đấu với nó bằng các sáng kiến chiến lược nhằm hiểu và cải thiện thế trận an ninh của mình.

Với môi trường kinh doanh phát triển nhanh chóng, cảnh quan về mối đe dọa mạng cũng đã thay đổi đáng kể trong năm qua. Điều này đang khiến các SMB trên toàn khu vực lo ngại hơn về rủi ro an ninh mạng. Ba phần tư (75%) SMB trong khu vực cho biết họ lo lắng hơn về an ninh mạng cách đây hơn 12 tháng, trong đó mối quan tâm lớn nhất là các SMB ở Ấn Độ (84%), Philippines (82%), New Zealand (81%), Indonesia (80%) và Australia (77%).

Những lo lắng đang được thúc đẩy một phần do nhận thức ngày càng nhiều về những tác động mà một sự cố nghiêm trọng có thể gây ra đối với công việc kinh doanh của họ. Ba phần tư (74%) các nhà lãnh đạo SMB được khảo sát cho biết một sự cố mạng lớn có thể đánh dấu sự kết thúc của tổ chức của họ.

Các SMB cũng ngày càng nhận thức được các mối đe dọa lớn nhất đến từ đâu. Nghiên cứu nhấn mạnh rằng lừa đảo được coi là mối đe dọa hàng đầu của các SMB trong khu vực,

với 43% xếp hạng đầu tiên. Lừa đảo là một chiến thuật mà tin tặc giả dạng là một thực thể đáng tin cậy để cố gắng và khiến người dùng mở một giao tiếp kỹ thuật số cụ thể được gửi cho họ, chẳng hạn như email, siêu liên kết hoặc tin nhắn tức thì. Mặc dù đây là một chiến thuật cũ nhưng nó vẫn được ưa chuộng do tính đơn giản và hiệu quả của nó. Đồng thời, môi trường phát triển nhanh chóng, do đại dịch gây ra, đã chứng kiến sự thay đổi lớn trong cách thức hoạt động của các SMB. Với sự thay đổi hàng loạt sang làm việc từ xa, một tỷ lệ khá lớn nhân viên đang kết nối với mạng của các công ty và truy cập thông tin từ bên ngoài văn phòng. Nhiều người cũng đang sử dụng thiết bị cá nhân để làm như vậy. Các SMB nhấn mạnh rằng máy tính xách tay không an toàn (20% xếp hạng 1), các cuộc tấn công có chủ đích bởi các tác nhân độc hại (19% xếp hạng 1) và thiết bị cá nhân (12% xếp hạng 1) là những mối đe dọa hàng đầu đối với bảo mật tổng thể của họ.

Những lo ngại mà các SMB thể hiện là có cơ sở. Hơn 4/5 các SMB trên khắp châu Á Thái Bình Dương cảm thấy bị phơi nhiễm trước các mối đe dọa mạng, trong đó 1/3 cảm thấy rất dễ bị ảnh hưởng. Điều này không kém phần quan trọng vì nhiều SMB đã trải qua sự cố mạng. Nghiên cứu cho thấy 56% SMB ở châu Á Thái Bình Dương đã gặp sự cố mạng trong 12 tháng qua.

Tuy nhiên, các con số khác nhau giữa các khu vực, với 74% SMB ở Ấn Độ và New Zealand gặp sự cố, trong khi chỉ 33% ở Indonesia và Hàn Quốc và 37% ở Nhật Bản cho biết họ bị sự cố. Ngoài ra, gần một nửa cho biết các sự cố mạng mà họ đã trải qua đã gia tăng trong thời kỳ đại dịch với Ấn Độ (70%) và New Zealand (61%) trải qua mức tăng lớn nhất, tiếp theo là Philippines (53%), Việt Nam (53%) và Úc (50%).

Nghiên cứu của Cisco cũng cho thấy 81% SMB đã thực hiện lập kế hoạch kịch bản hoặc mô phỏng cho các sự cố an ninh mạng tiềm ẩn trong 12 tháng qua. Đa số SMB (81%) có sẵn kế hoạch ứng phó trong khi 82% có kế hoạch khôi phục sẵn sàng triển khai nếu cần.

Nằm trong khu vực sôi động nhất của khu vực châu Á Thái Bình Dương về chuyển đổi số, các SMB ở Việt Nam ngày càng nhận thức rõ hơn về các rủi ro an ninh mạng

hiện tại và họ đang đầu tư nhiều hơn để có sự chuẩn bị tốt khi gặp sự cố mạng.

Theo nghiên cứu của Cisco tại riêng thị trường Việt Nam, 71% các SMB tại Việt Nam cho biết họ quan tâm hơn đến an ninh mạng so với 12 tháng trước. 89% SMB tại Việt Nam có kế hoạch ứng phó trên không gian mạng đối với các sự cố tiềm ẩn.

Hình ảnh và số liệu trích xuất từ bản nghiên cứu

Nghiên cứu cũng cho biết khoảng 59% SMB trên lãnh thổ Việt Nam gặp sự cố mạng trong 12 tháng qua. Gần 1/3 (30%) nói rằng những sự cố mạng này khiến doanh nghiệp của họ thiệt hại hơn 500.000 USD. 86% những người ở Việt Nam bị sự cố mạng bị mất thông tin khách hàng. Nguyên nhân số một gây ra những sự cố này là do các giải pháp an ninh mạng không đủ khả năng phát hiện hoặc ngăn chặn cuộc tấn công. Những cuộc tấn công này có tác động rõ rệt đến các SMB - từ sự gián đoạn trong hoạt động, thiệt hại doanh thu cho tới tác động tiêu cực đến uy tín của tổ chức.

Nhiều công ty đã chuyển hướng sang làm việc kết hợp do đại dịch, điều này đã dẫn đến phần lớn nhân viên kết nối với mạng của các tổ chức và truy cập thông tin từ bên ngoài văn phòng, trong đó nhiều người sử dụng thiết bị cá nhân để làm việc này. Theo các SMB tại Việt Nam tham gia khảo sát, những chiếc máy tính xách tay không được bảo mật, các cuộc tấn công có chủ đích của tin tặc và việc sử dụng thiết bị cá nhân là những mối đe dọa hàng đầu đối với an ninh chung của tổ chức.

Bà Lương Thị Lệ Thủy, Tổng Giám đốc Cisco Việt Nam cho biết: *"Việc áp dụng công nghệ nhiều hơn cũng đồng nghĩa với việc ngày càng có nhiều nguy cơ tấn công an ninh mạng do bề mặt tấn công được mở rộng. Khi các SMB tại Việt Nam đẩy nhanh quá trình số hóa để cung cấp các ứng dụng thế hệ tiếp theo và cải tiến hình thức làm việc kết hợp trong giai đoạn bình thường mới, thì việc đảm bảo rằng tổ chức của họ được bảo vệ trên mọi mặt sẽ tiếp tục là ưu tiên hàng đầu."*

Đánh giá chính xác rủi ro mới có thể phản ứng nhanh

Khi các SMB trên toàn khu vực chuẩn bị cho một tương lai công việc kết hợp, với việc các nhân viên phân tán giữa công việc tại văn phòng và làm việc từ xa, điều này làm tăng thêm một lớp phức tạp khác để giải quyết vấn đề an ninh mạng.

An ninh mạng giống như một trò chơi cá cược mà thực tế là tỷ lệ cược nghiêng về những kẻ gây hại. Chúng liên tục tấn công các mục tiêu đã nhắm đến. Những người bị tấn công cần phải giành chiến thắng trong mọi thời điểm. Còn những kẻ tấn công chỉ cần vượt qua hàng phòng ngự một lần để giành chiến thắng. Thêm vào đó, thực tế là phải mất một thời gian để các công ty phát hiện, điều tra và khắc phục sự cố mạng.

Thách thức mà các SMB đang phải đối mặt là chúng ta đang sống trong một thế giới siêu kết nối, ưu tiên kỹ thuật số, nơi khách hàng muốn có sự hài lòng tức thì. Điều này có nghĩa là họ có rất ít thời gian, nếu có, để khắc phục một sự cố an ninh mạng có thể làm gián đoạn hoạt động của mình. Họ cần có khả năng phát hiện, điều tra và ngăn chặn hoặc khắc phục mọi sự cố mạng càng nhanh càng tốt. Nghiên cứu của Cisco nhấn mạnh rằng 15% SMB ở châu Á Thái Bình Dương nói rằng thời gian ngừng hoạt động thậm chí dưới một giờ sẽ dẫn đến gián đoạn hoạt động, trong khi 29% cho biết thời gian ngừng hoạt động từ 1 đến 2 giờ có thể gây ra tình trạng tương tự. Tác động có thể được định lượng vì 13% số người được hỏi cho biết thời gian ngừng hoạt động dưới một giờ sẽ ảnh hưởng nghiêm trọng đến doanh thu, trong khi 24% cho biết thời gian ngừng hoạt động từ 1 đến 2 giờ có thể gây ra điều tương tự. Điều đáng nói nhất là một trong 10 SMB cho biết thời gian ngừng hoạt động trong một ngày sẽ dẫn đến việc đóng cửa tổ chức của họ.

Đồng thời, khi các quốc gia bắt đầu đưa ra và thực hiện các hướng dẫn và quy định về an ninh mạng, thời gian ngừng hoạt động do các sự cố mạng cũng dẫn đến các tác động pháp lý. Xu hướng này đã bắt đầu xuất hiện, với 13% SMB cho biết thời gian ngừng hoạt động dưới một giờ sẽ có ý nghĩa pháp lý đối với họ, trong khi 22% cho biết thời gian ngừng hoạt động từ 1 đến 2 giờ có thể gây ra điều tương tự. Thách thức lớn đối với các SMB là chỉ có 15% số người được hỏi cho biết họ có thể phát hiện ra sự cố mạng trong vòng một giờ. Số người có thể khắc phục sự cố trong vòng một giờ thậm chí còn thấp hơn ở mức 10%.

Tốc độ phản ứng với một sự cố trở nên quan trọng do tác động của phản ứng chậm chạp có thể có đối với doanh nghiệp. Nó không chỉ là mất doanh thu mà các SMB còn phải vật lộn với tác động tổng thể. Hơn một nửa (51%) SMB trong khu vực bị sự cố mạng trong 12 tháng qua cho biết những sự cố này khiến doanh nghiệp thiệt hại từ 500.000 đô la Mỹ trở lên, với 13% cho rằng chi phí này là hơn 1 triệu đô la Mỹ. Trên thực tế, phần lớn những người bị một sự cố đều có tác động về mặt tiền bạc. Nhìn chung, 83% cho biết chi phí cho các sự cố là hơn 100.000 đô la Mỹ. Ngoài ra còn có chi phí vô hình. Trong số những người bị sự cố trong năm qua, 57% nói rằng nó dẫn đến mất niềm tin với khách hàng, trong khi 66% nói rằng nó ảnh hưởng tiêu cực đến danh tiếng của họ. Mặc dù không thể chứng minh được, sự suy giảm danh tiếng và xói mòn lòng tin có thể gây ra những hậu quả tai hại cho bất kỳ doanh nghiệp nào.

Chính vì những lý do trên, an ninh mạng đã trở thành một lĩnh vực trọng tâm chính của các tổ chức, doanh nghiệp khi họ áp dụng hình thức làm việc kết hợp (Hybrid work), cho phép nhân viên làm việc an toàn từ mọi nơi và thông qua các thiết bị khác nhau. Điều này đã mở rộng bề mặt tấn công và gia tăng rủi ro an ninh mạng, vượt ngoài phạm vi bảo vệ của các doanh nghiệp. Đây cũng là khó khăn lớn nhất của các SMB trong công tác đánh giá toàn diện rủi ro an ninh mạng trước khi xác lập chính sách và đầu tư giải pháp an toàn thông tin. Từ thực tế này, Cisco đã cho ra mắt Công cụ Đánh giá an ninh mạng mới, cho phép các SMB hiểu rõ hơn về tình hình bảo mật tổng thể của doanh nghiệp.

"Là bước đầu tiên trong quá trình áp dụng chiến lược bảo vệ an ninh mạng trên toàn bộ hệ thống thông tin, các SMB có thể sử dụng công cụ đánh giá trực tuyến mới của Cisco nhằm giúp họ cải thiện khả năng phục hồi bằng cách cung cấp kiến thức về mức độ chuẩn bị cho an ninh mạng cũng như các cơ hội và lỗ hổng cần được lưu ý", bà Lương Thị Lệ Thủy cho biết thêm.

Công cụ đánh giá trực tuyến mới đánh giá "mức độ sẵn sàng về an ninh mạng" của từng tổ chức thông qua phương pháp tiếp cận "Zero Trust", nghĩa là tất cả mọi nỗ lực truy cập vào cấu trúc mạng của một tổ chức đều không được chấp nhận cho đến khi có thể xác minh được độ tin cậy. Khi người dùng truy cập ứng dụng bằng bất cứ thiết bị nào, cả người dùng và thiết bị sẽ được xác minh và giám sát liên tục. Điều này giúp bảo vệ các ứng dụng và môi trường của tổ chức khỏi bất cứ người dùng, thiết bị và từ vị trí nào.

Công cụ này đánh giá mức độ trưởng thành của tổ chức trong sáu khía cạnh của Zero Trust, bao gồm: Người dùng và Danh tính, Thiết bị, Mạng, Khối lượng công việc (ứng dụng), Dữ liệu và Vận hành bảo mật. Sau khi tổ chức nhập thông tin chi tiết về các chính sách và khả năng bảo mật của mình, công cụ này sẽ đánh giá tình hình bảo mật tổng thể của tổ chức dựa trên các tiêu chuẩn ngành và lĩnh vực.

Công cụ này tổng hợp báo cáo riêng cho từng tổ chức, cho biết mức độ trưởng thành, thách thức và cơ hội của họ trong từng khía cạnh trong sáu khía cạnh của Zero Trust. Ngoài ra, công cụ này còn có thể đưa ra các khuyến nghị phù hợp về công nghệ và giải pháp giúp tăng cường vị thế và khả năng sẵn sàng về an ninh tổng thể của tổ chức trong một môi trường làm việc kết hợp.

Trong một thế giới ngày càng chuyển đổi sâu hơn vào không gian số, các SMB phải đầu tư ngày càng nhiều thời gian và nguồn lực để quản lý không gian này và vượt qua các rào cản an ninh mạng của mình nhằm xây dựng một doanh nghiệp linh hoạt, có khả năng chống lại các rủi ro trong tương lai để đạt tới thành công. ■ THÔNG TIN & TRUYỀN THÔNG

Tài liệu tham khảo:

1. *https://www.cisco.com/c/en_sg/products/security/cybersecurity-for-smbs-in-asia-pacific/index.html*
2. *https://www.cisco.com/c/en/us/products/security/zero-trust.html*
3. *https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/3051495/extending-zero-trust.pdf?dtid=osscdc000283*