AN NINH MẠNG
THÀNH TỐ QUAN TRỌNG TRONG CHUYỂN ĐỔI SỐ

TS. HOÀNG SỸ TƯƠNG *, TS. NGUYỄN TÂN ĐĂNG **

**, ** Học viện Kỹ thuật Mật mã – Ban Cơ yếu Chính phủ*

Chuyển đổi số đang thay đổi hoạt động sản xuất kinh doanh của mọi tổ chức, thông qua các công nghệ mới giúp mở ra lợi thế cạnh tranh, mang lại sự hiệu quả, linh hoạt và nâng cao trải nghiệm của khách hàng. Với tình hình các mối đe dọa về an ninh thông tin ngày càng gia tăng, việc Chuyển đổi số sẽ không thể thành công nếu không xây dựng một chiến lược an ninh mạng phù hợp.

Chuyển đổi số đang có những tác động mạnh mẽ đến cấu trúc cũng như cách thức hoạt động và cách thức tổ chức của doanh nghiệp. Cloud, IoT, Big Data và các vấn đề về tính di động đang tạo ra sự phát triển nhanh chóng của các mô hình, cơ sở hạ tầng và việc sử dụng các nền tảng công nghệ thông tin. Có thể nói chúng ta đang kết nối với nhau nhiều hơn bao giờ hết. Điều thú vị là, mặc dù 58% các công ty coi chuyển đổi số là vấn đề quan trọng thứ 2 đối với doanh nghiệp, chỉ đứng thứ hai sau vấn đề doanh thu, nhưng chỉ có 7% các tổ chức coi an ninh mạng là vấn đề ưu tiên hàng đầu trong chuyển đổi số của các công ty. Vậy tại sao, trong khi các nguy cơ về vi phạm an ninh mạng tiếp tục gia tăng thông qua việc chuyển đổi số, thì các giải pháp an ninh tốt giúp cải thiện vấn đề an ninh mạng lại không được áp dụng một cách kịp thời để đối phó với các đe doạ tấn công ngày càng gia tăng?

Có rất nhiều câu trả lời cho câu hỏi này. Thứ nhất, có thể việc giám sát các nguy cơ thông qua việc chỉ sử dụng các nguồn lực nội bộ là rất khó khăn bởi vì tính phức tạp và khả năng thay đổi nhanh chóng của các tấn công. Cần phải lường trước các cuộc tấn công thay vì chỉ đơn giản là bảo vệ tổ chức khi các tấn công đã xảy ra. Thứ hai, các vấn đề an ninh đôi khi bị bỏ qua vì những ảnh hưởng to lớn của một cuộc tấn công không được tính đến khi ước tính thiệt hại mà nó gây ra. Thứ ba, cho rằng hệ thống của bạn không dễ dàng bị tổn thương. Một số tổ chức tin rằng nguy cơ mà họ trở thành nạn nhân của một cuộc tấn công mạng là khá nhỏ. Nhưng họ đã sai lầm, trên thực tế, các lỗ hổng trong dữ liệu của họ khiến cho các doanh nghiệp vừa và nhỏ trở thành mục tiêu tấn công của hacker, đặc biệt là các tấn công mã hóa dữ liệu.

Các rủi ro an ninh mạng trong kỷ nguyên chuyển đổi số

Công nghệ đang thúc đẩy sự phát triển của cuộc sống, xã hội và tác động của nó vào việc chuyển đổi số như thế nào?

Vai trò của công nghệ đối với cuộc sống của con người đang trở thành một chủ đề bàn luận sâu rộng trong xã hội hiện nay. Xem xét bản chất và tốc độ thay đổi của công nghệ cũng như sự khác biệt của nó hiện nay so với giai đoạn trước đây là điều cần phải được làm rõ. Nhìn lại 20 trước, Internet, WWW, chỉ mới ở giai đoạn sơ khai. Các công ty như AOL, có một cổng Web và nhà cung cấp dịch vụ trực tuyến, được xem là ông trùm của lĩnh vực truyền thông, CD là ông vua của ngành công nghiệp ghi âm. Nokia vừa ra mắt điện thoại di động màn hình đơn sắc đầu tiên trên thế giới, và đám mây chỉ được biết đến như những gì mọi người vẫn nhìn thấy trên bầu trời. Ngày nay, có hơn 4,1 tỉ người dùng Internet, hơn 1,8 tỉ trang web và hơn 337 tỷ GB lưu lượng truy cập Internet chỉ tính riêng trong năm nay – trong đó 52% được tạo ra thông qua điện thoại di động. Và đó chưa phải là tất cả, theo Paul Daugherty, Giám đốc Công nghệ & Đổi mới sáng tạo tại Accenture, sổ cái phân tán, AI, công nghệ thực tế mở rộng, và tính toán lượng tử là những công nghệ lớn tiếp theo cho sự thay đổi trong những năm tới.

Những tiến bộ trong công nghệ mà chúng ta đang thấy hiện nay đang phát triển nhanh chóng, điều này thể hiện rõ hơn khi ngày càng có nhiều dữ liệu có giá trị hơn. Khi công nghệ tiếp tục thích ứng và phát triển với tốc độ vượt xa nền văn hóa và thể chế của chúng ta, các tổ chức không cân nhắc về an ninh mạng trong chiến lược chuyển đổi số sẽ gặp rủi ro lớn, vì sự trì trệ này sẽ dẫn đến những bất ổn cho tổ chức. Khi động lực hướng tới chuyển đổi số tiếp tục gia tăng không ngừng, đây là thời điểm thích hợp để các tổ chức tạm dừng lại và suy nghĩ một cách thấu đáo về chiến lược an ninh mạng của mình.

Làm thế nào để an ninh mạng có thể đảm bảo cho việc chuyển đổi số thành công?

Khả năng định hình lại các quy trình kỹ thuật số và các chức năng được xác định phần lớn thông qua chiến lược số được hỗ trợ bởi các nhà lãnh đạo của các tổ chức, những người thúc đẩy văn hóa và truyền cảm hứng cho sự thay đổi và đổi mới sáng tạo. Trong khi những hiểu biết sâu sắc về chuyển đổi số phù hợp với những phát triển công nghệ trước đây, nhưng điều đặc biệt của chuyển đổi số hiện nay là việc chấp nhận rủi ro như là một chuẩn mực văn hóa khi các công ty kỹ thuật số hàng đầu tìm kiếm những con đường mới để tạo ra các lợi thế cạnh tranh. Trong môi trường công nghệ ngày nay, sự tự tin trong việc có được lợi thế cạnh tranh phần lớn là do an ninh mạng và quản lý dữ liệu để tận dụng tối đa môi trường số. Trong thời đại của các phân tích và trí tuệ, việc cạnh tranh trong một thế giới dựa vào dữ liệu là rất khó khăn. Sẽ không quá lời khi nói rằng môi trường kinh doanh ngày nay đã trở nên siêu cạnh tranh và các tổ chức không liên tục tái tạo lại hoạt động kinh doanh của mình với dữ liệu đóng vai trò cốt lõi chắc chắn sẽ đi chệch hướng, phải đứng ngoài lề trong khi thị trường kinh doanh bị gián đoạn. Tuy nhiên, khi kỹ thuật số được xây dựng cho mục đích phân tích, các công ty phải rất khó khăn trong việc đại tu và thay đổi các hệ thống hiện có.

Khi công nghệ phát triển, mức độ rủi ro an ninh mạng cũng tăng theo. Theo một báo cáo của Deloitte, các nhà phân tích ước tính rủi ro mạng toàn cầu "có thể làm chậm tốc độ đổi mới công nghệ tới 3 nghìn tỷ USD giá trị kinh tế bị mất trong năm 2020". Các điểm yếu trong tổ chức đối với các mối đe doạ từ mạng có thể giảm thiểu bằng cách phát triển các chiến lược an ninh mạng mạnh mẽ, đó là điều tối quan trọng đối với công ty, để tự tin quản lý khả năng phục hồi trên không gian mạng. Đầu tư vào an ninh mạng cho phép các tổ chức hiểu được mức độ hồi phục trên không gian mạng trên cơ sở các tài sản kinh doanh quan trọng, bối cảnh đe dọa đối với họ và mức độ phát triển khả năng phòng thủ không gian mạng của họ. Hơn nữa, các tích hợp cho phép các tổ chức theo dõi mức độ hồi phục trên không gian mạng và có thể tùy chỉnh cho các đối tượng hoạt động, quản lý và điều hành. Việc triển khai hiệu quả giúp khắc phục tình trạng mất cân bằng của tổ chức và thể hiện bức tranh toàn cảnh về doanh nghiệp được bảo vệ trên không gian mạng bằng cách sử dụng các tiêu chuẩn an toàn, chính sách và thực hành, tăng cường hợp tác và chia sẽ thông tin cũng như tăng cường hợp tác giữa các đối tác với nhau.

Một số giải pháp quan trọng đảm bảo an ninh mạng cho chuyển đổi số

Mathieu Poujol, Cố vấn chính của PAC France, CXP Group, công ty tư vấn độc lập hàng đầu của châu Âu trong lĩnh vực phần mềm dịch vụ công nghệ thông tin và chuyển đổi số giải thích: *"Thị trường an ninh mạng là một trong những thị trường tăng trưởng nhanh nhất ở châu Âu, đặc biệt là các công ty lớn. Tuy nhiên xu hướng tăng trưởng này rất rộng vì 25% tổ chức đã áp dụng chính sách không cần giấy tờ cho hội đồng quản trị của các công ty trên phạm vi toàn thế giới"*. An ninh mạng, được thúc đẩy bởi sự tăng trưởng nội tại của ngành công nghiệp số, hiện đang là một thị trường quan trọng. Dự đoán năm 2021, có khoảng 50% thành viên hội đồng quản trị sẽ chọn chuyển sang không dùng giấy tờ. Nhưng ngoài sự lớn mạnh của ngành an ninh mạng, chính con người, lãnh đạo các hội đồng quản trị và các thành viên tại nơi làm việc phải thay đổi thói quen của họ. Đây là những mục tiêu dễ bị tấn công nhất trong công ty vì họ là những người đang sở hữu các thông tin tuyệt mật của công ty.

Hình thành chiến lược đảm bảo an ninh cho đội ngũ lãnh đạo

Bằng cách sử dụng các môi trường ảo và an toàn, chúng ta có thể ngăn chặn được các hậu quả của các cuộc tấn công mạng đối với toàn bộ chuỗi giá trị của công ty. An ninh mạng là điều cần thiết và có vai trò quan trọng nhìn từ góc độ chuyên môn và kinh doanh. Nếu tiếp cận vấn đề theo cách này; chiến lược được đưa ra phải dưới dạng một lộ trình. Ví dụ, bảo mật dữ liệu của hội đồng quản trị phụ thuộc vào cách sử dụng chung của cả nhóm. Việc áp dụng cách tiếp cận "an toàn thông qua thiết kế" giúp lường trước các rủi ro của các cuộc tấn công mạng. Việc áp dụng giải pháp quản lý đối với dữ liệu, các cuộc họp và các tài liệu có nghĩa là phải lường trước được các rủi ro về an ninh mạng. Có nhiều lợi thế để phát triển theo hướng sử dụng văn phòng không giấy tờ. Hiệu quả lãnh đạo trong hội đồng quản trị được tăng cường: ngược lại việc chuẩn bị cho các cuộc họp trở nên đơn giản hóa ở cấp độ quản lý dữ liệu và cấp quyền truy cập. Việc sử dụng các máy chủ theo chuẩn ISO 27001 giúp bảo vệ hội đồng quản trị khỏi các vi phạm có thể xảy ra. Văn phòng không giấy tờ cũng cung cấp các trải nghiệm thú vị hơn cho các thành viên của hội đồng quản trị. Trên thực tế, quyền truy cập dữ liệu, tính di động của các tài liệu và sử dụng các công cụ hợp tác có thể giúp đưa ra quyết định nhanh hơn và chính xác hơn. Để đảm bảo việc quản lý hiệu quả và thực hiện các quyết định một cách nhanh chóng, điều cần thiết là phải có một giải pháp phù hợp, linh hoạt và dễ áp dụng. Bởi vì sự thật là không thể tồn tại nền kinh tế số mà không có sự hiện diện của an ninh số.

Phân tích rủi ro về các vấn đề an ninh mạng

Không có gì là bí mật khi chi phí tài chính của một cuộc tấn công mạng đủ lớn để làm tê liệt hoạt động kinh doanh của một doanh nghiệp vừa và nhỏ. Ngoài những tác động tiêu cực về mặt tài chính, giá trị thương hiệu cũng bị suy giảm không kém khi khách hàng thấy quyền riêng tư của họ bị xâm phạm, làm thay đổi lòng tin của khách hàng và làm giảm uy tín của thương hiệu. Số vụ vi phạm dư liệu do các công ty dịch vụ tài chính của Anh báo cáo cho cơ quan kiểm toán tài chính (FCA) đã tăng 480% vào năm 2020 lên 145 vụ, tăng so với chỉ 25 vụ vào năm 2019. Các tổ chức phải vật lộn để theo kịp với sự tấn công của cộng đồng tội phạm mạng. Theo báo cáo của Forbes, các doanh nghiệp ưu tiên cho vấn đề an ninh mạng đang tạo ra lợi thế cạnh tranh đáng kể so với với các doanh nghiệp cùng lĩnh vực. Kỹ thuật số đang phát triển mạnh mẽ cũng với công nghệ và đang đang cung cấp nhiều dữ liệu cá nhân hơn bao giờ hết, bất chấp các rủi ro và hậu quả về vấn đề an ninh mạng ngày càng gia tăng. Một nghiên cứu của Experian cho biết 70% khách hàng trên toàn cầu *"sẵn sàng chia sẻ dữ liệu cá nhân với các tổ chức mà họ đang tương tác trực tuyến, đặc biệt là khi họ thấy có lợi"*. Một cuộc khảo sát khác do trung tâm đổi mới dữ liệu đưa ra cũng cho thấy 58% khách hàng *"sẵn sàng chia sẽ các dữ liệu cá nhân nhạy cảm"* (ví dụ, sinh trắc học, dữ liệu y tế/nơi cư trú) để đổi lấy việc sử dụng một số ứng dụng và dịch vụ. Người tiêu dùng đang đặt niềm tin vào các tổ chức để quản lý và bảo vệ dữ liệu cá nhân của họ và các tổ chức phải được trang bị tốt về chiến lược an ninh mạng để bảo vệ

khách hàng của mình. Thách thức phổ biến nhất và sự cần thiết để vượt qua các nguy cơ tấn công mạng là phải kết hợp an ninh vào một tầm nhìn chiến lược chung. Bước tiếp theo là phát triển các quy trình kinh doanh phù hợp và xây dựng các khả năng, bao gồm cả hạ tầng dữ liệu và nguồn nhân lực chất lượng cao. Nếu chỉ đơn giản là sắp xếp lại các hệ thống công nghệ để ra tăng sức mạnh cho các hoạt động kinh doanh hiện có là chưa đủ. Tất cả các khía cạnh phải chuyển đổi này cần được kết hợp với nhau để giúp nhận ra tiềm năng đầy đủ của an ninh mạng.

Nhúng an ninh mạng vào chuyển đổi số

Điều quan trọng đối với các tổ chức là đặt vấn đề bảo mật như là điểm khởi đầu của công việc chuyển đổi số. Bất chấp số lượng lớn các vụ vi phạm dữ liệu trên toàn cầu, an ninh mạng vẫn là một vấn đề cần phải cân nhắc đối với phần lớn các hoạt động chuyển đổi số mà các doanh nghiệp đang thực hiện hiện nay như: tính di động, dịch vụ đám mây và các chương trình trải nghiệm của khách hàng. Thật không may, vấn đề an ninh mạng được coi là nguyên nhân làm chậm dự án, thay vì tạo điều kiện cho nó phát triển. Tuy nhiên, có thể hiểu được, với áp lực về thời gian để bắt đầu thực hiện dự án, việc thiếu cân nhắc hợp lý về vấn đề an ninh mạng là một vấn đề đối với các tổ chức để cải thiện khả năng phục hồi mạng và an ninh mạng. Rõ ràng là trong môi trường số hóa ngày nay, với tần suất ngày càng tăng và công khai của các cuộc tấn công mạng và độ phức tạp ngày càng cao của nó, các doanh nghiệp phải biết rằng khách hàng của họ ngày càng có nhận thức rõ hơn về vấn đề an ninh mạng. Việc áp dụng chiến lược an ninh mạng vào thời điểm này là một lợi thế cạnh tranh quan trọng. Theo một khảo sát của các chuyên gia công nghệ thông tin và bảo mật chỉ có 18% các tổ chức đồng ý rằng nhóm bảo mật của họ đã tham gia vào tất cả các dự án chuyển đổi số và 76% đồng ý rằng xem xét về vấn đề an ninh mạng đã được thêm quá muộn vào trong dự án, cuối cùng dẫn đến kết quả là các dự án bị trì hoãn do được trang bị thêm về an ninh mạng sau khi các quyết định quan trọng đã được đưa ra. Trong cùng một cuộc khảo sát, 85% số người được hỏi đồng ý rằng đội an ninh mạng có thể đã hoàn thành tốt công việc của họ nếu họ được tham gia sớm trong các dự án. Thách thức chính và mục tiêu tổng thể đối với nhóm an ninh mạng là việc trấn an tổ chức rằng cơ sở hạ tầng công nghệ thông tin của họ là an toàn và có khả năng phục hồi. Tuy nhiên, điều quan trọng là các tổ chức phải hiểu rằng không có dự án chuyển đổi số nào được bắt đầu thực hiện mà không hiểu rõ về tác động an ninh mạng đối với chúng. Các tổ chức khai thác khả năng này một cách hiệu quả có thể tạo ra giá trị thặng dư và tạo ra sự khác biệt cho chính họ, trong khi những tổ chức khác sẽ ngày càng thấy mình ở vào thế bất lợi. Hơn bao giờ hết, tất cả chúng ta đang phụ thuộc rất nhiều vào nền kinh tế số mới nổi này. Và khi các tổ chức, các cơ quan chính phủ và cơ sở hạ tầng quan trọng của chúng ta chuyển sang mô hình số, một sự kiện an ninh mạng xảy ra có thể gây hậu quả thảm khốc cho tất cả chúng ta. Cũng cần nhớ rằng các sự kiện an ninh mạng xảy ra không dựa trên các vấn đề chính trị, xã hội hoặc kinh tế. Khi một cơ sở hạ tầng hoặc hệ thống kinh tế bị tấn công và bị tổn hại mọi người đều phải gánh chịu hậu quả.

Kết luận

Để có thể có được môi trường an toàn, an ninh mạng vững chắc song hành cùng hành trình chuyển đổi số, các tổ chức và các doanh nghiệp cần phải xây dựng chiến lược an ninh mạng cụ thể cho đội ngũ lãnh đạo, thực hiện phân tích rủi ro an ninh mạng trước khi triển khai các dự án cũng như nhúng an ninh mạng vào quá trình chuyển đổi số. Đồng thời cũng cần phải tăng cường đầu tư nguồn lực tài chính cho lĩnh vực này và xây dựng một đội ngũ chuyên gia về an toàn, an ninh mạng làm nòng cốt. Các bộ phận an ninh mạng của các tổ chức và công ty cần làm chủ công nghệ, có những cách tiếp cận mới về sản phẩm để nhanh chóng phát hiện và ngăn chặn những cuộc tấn công ngày càng phức tạp và nguy hiểm, để giúp quá trình chuyển đổi số của các tổ chức và doanh nghiệp diễn ra thành công. ■

Tài liệu tham khảo:

1. Sheila Pancholi, Gregor Strobl, Digital transformation and its impact on cybersecurity – 2019.

2. Capgemini, No digital transformation without cyber security - 2020.

3. Anh Nguyen Duc, Aparna Chirumamilla, Identifying Security Risks of Digital Transformation - An Engineering Perspective - 2019.

4. Patrick Hoberg, Helmut Krcmar, Bernd Welz, Skills for Digital Transformation: Research Report 2017.