Tiêu đề: An ninh mạng trong thời đại mới
Tác giả: CK – Nguồn: TTTCTT đăng ngày 22-10-2020
Đường dẫn bài viết: https://thitruongtaichinhtiente.vn/an-ninh-mang-trong-thoi-dai-moi-31317.html

An ninh mạng trong thời đại mới

(thitruongtaichinhtiente.vn) - An ninh mạng đang nắm giữ vị trí then chốt đối với nhiều ngành công nghiệp, các tổ chức và từng cá nhân người dùng. Đồng thời, ngày một khẳng định vai trò là yếu tố hỗ trợ thiết yếu đối với doanh nghiệp.

Đây là kết quả nổi bật từ cuộc Khảo sát "Niềm tin kỹ thuật số 2021 - Digital Trust Insights 2021" do PwC thực hiện. Khảo sát mang đến phân tích chuyên sâu về những thay đổi và xu hướng phát triển an ninh mạng trong tương lai. Khảo sát ghi nhận ý kiến của trên 3.000 lãnh đạo doanh nghiệp và lãnh đạo công nghệ trên toàn thế giới.

Chia sẻ về báo cáo, bà Nguyễn Phi Lan, Lãnh đạo dịch vụ Tư vấn Quản lý Rủi ro tại PwC Việt Nam cho biết: "Khảo sát lần này ghi nhận 96% các lãnh đạo cấp cao dự kiến sẽ điều chỉnh an ninh mạng do ảnh hưởng của COVID-19, đồng thời 50% cho biết có khả năng doanh nghiệp sẽ cân nhắc vấn đề an ninh mạng khi đưa ra mọi quyết định kinh doanh (con số tăng từ

25% so với báo cáo năm ngoái). Có thể thấy, vai trò của các CISO đối với doanh nghiệp đang thay đổi và ngày càng trở nên quan trọng hơn bao giờ hết. Các Giám đốc điều hành và ban lãnh đạo cần sự hỗ trợ từ các CISO để nâng cao khả năng thích ứng của doanh nghiệp và tạo ra giá trị kinh doanh. Nhiều doanh nghiệp đang bắt tay vào tái khởi động các chiến lược về an ninh mạng".

Trước những tác động của COVID-19 tới nền kinh tế thế giới, các doanh nghiệp đang chuyển đổi dần mô hình kinh doanh và cũng đẩy nhanh việc áp dụng các chương trình kỹ thuật số. Báo cáo của PwC phân tích năm yếu tố các Giám đốc an toàn thông tin (CISO) cần cân nhắc thực hiện để vượt qua giai đoạn thử thách này và có những bước tiến trong tương lai.

Nhu cầu cấp thiết về nâng cấp chiến lược an ninh mạng: Song hành với các công nghệ và mô hình kinh doanh mới – cùng tốc độ ứng dụng nhanh chóng – là những rủi ro mới. Trong 3 tháng đầu khi đại dịch bùng phát, các giám đốc điều hành (CEO) cho biết doanh nghiệp của họ đang tăng tốc số hóa ở mức độ đáng ngạc nhiên, đẩy nhanh tiến độ tới 2 hoặc 3 năm trong kế hoạch 5 năm theo dự kiến. Tối ưu hóa hiệu quả và tốc độ làm việc là tham vọng hàng đầu đối với 29% các lãnh đạo, trong khi đó 31% ưu tiên hiện đại hóa thông qua việc phát triển các năng lực mới.

Cân nhắc lại ngân sách an ninh mạng: Tối ưu hóa hiệu quả an ninh mạng so với chi phí bỏ ra là bài toán ngày càng quan trọng đối với các doanh nghiệp khi số hóa: mỗi quy

trình và tài sản số mới đều có thể trở thành lỗ hổng mới cho tấn công mạng. Hơn một nửa các doanh nghiệp được khảo sát (55%) tuyên bố sẽ tăng cường ngân sách an ninh mạng vào năm 2021. Tuy đây là thông tin tích cực, vấn đề quản lý ngân sách cho an ninh mạng dự kiến sẽ cần những thay đổi trong tương lai.

Với Việt Nam, ông Phó Đức Giang, Giám đốc Công ty TNHH Dịch vụ An toàn Thông tin PwC Việt Nam nhận xét: "Thời gian gần đây tại Việt Nam đã có những khoản tăng đầu tư tương tự cho an ninh mạng cụ thể về giải pháp kỹ thuật, quản lý dịch vụ mạng và nguồn nhân lực. Tuy nhiên, theo quan sát của chúng tôi, rất ít công ty đang vận hành các quy trình chuẩn về lượng hóa rủi ro an ninh mạng. Bên cạnh đó, các lãnh đạo an ninh mạng tại Việt Nam cần có thông tin đầy đủ hơn về kế hoạch kinh doanh của doanh nghiệp để tự tin hơn trong việc dự toán ngân sách cũng như trong quá trình ra quyết định".

Đối mặt với tấn công an ninh mạng: Các sáng kiến và công nghệ đang thay đổi cách doanh nghiệp đối mặt và san bằng sân chơi đối với tội phạm tấn công an ninh mạng. 43% lãnh đạo được khảo sát cho biết doanh nghiệp của họ đã cải thiện trải nghiệm khách hàng và đang ứng phó nhanh nhạy hơn khi xảy ra sự cố hay gián đoạn. Các kết quả được các lãnh đạo kỳ vọng nhất trong 2-3 năm tới bao gồm: tăng số lần ngăn chặn thành công các vụ tấn công mạng, rút ngắn thời gian ứng phó khi xảy ra gián đoạn, nâng cao niềm tin vào năng lực lãnh đạo để xử lý các mối đe dọa, và nâng cao trải nghiệm khách hàng.

Xây dựng khả năng thích ứng: Gia tăng quy mô và tốc độ số hóa đồng nghĩa với bề mặt tấn công lớn hơn và tiềm ẩn nhiều nguy cơ hơn đối với doanh nghiệp. 2020 là một năm có rất nhiều những "lần đầu tiên": đối với nền kinh tế, sức khỏe cộng đồng và các tổ chức an ninh mạng. Đã có sự tăng vọt về số lượng các vụ tấn công xâm nhập, mã độc tống tiền (ransomware) và rò rỉ dữ liệu trong các tổ chức giáo dục và y tế, cũng như số lượng các vụ tấn công giả mạo.

40% các lãnh đạo được khảo sát cho biết có kế hoạch tăng cường kiểm tra khả năng phục hồi để đảm bảo các dịch vụ kinh doanh quan trọng được duy trì ngay cả khi xảy ra sự cố mạng gây gián đoạn.

"Trong một vài năm trở lại đây, ngày càng nhiều công ty hướng đến phát triển và cung cấp các dịch vụ hệ sinh thái tới khách hàng" ông Phó Đức Giang nhận định. "Để nhanh chóng đạt được điều này, một trong những phương pháp được nhiều công ty áp dụng là kết nối hệ thống cốt lõi của doanh nghiệp với hệ thống của bên thứ ba khác hoặc sử dụng bên thứ ba để cung cấp các dịch vụ tạo giá trị gia tăng cho khách hàng. Tuy nhiên, những hoạt động thông qua bên thứ ba hoặc bên thứ tư như vậy tiềm ẩn nhiều nguy cơ rò rỉ dữ liệu. Do đó, việc lên kế hoạch kiểm tra và đánh giá khả năng phục hồi cần thiết cho doanh nghiệp là rất quan trọng".

Chuẩn bị đội ngũ cho tương lai: Với dự báo sẽ có tới 3,5 triệu việc làm liên quan tới an ninh mạng vào năm 2021, trăn trở lớn nhất đối với toàn ngành an ninh mạng là vấn đề thiếu hụt nguồn nhân lực có kỹ năng. 51% lãnh đạo tham gia khảo sát cho biết có kế hoạch tuyển dụng nhân sự toàn thời gian cho an ninh mạng trong năm sau, với hơn 22% dự kiến gia tăng nhân sự từ 5% trở lên.

Giải pháp khác mà nhiều doanh nghiệp lựa chọn cho các vị trí còn trống là "tuyển dụng từ bên trong". Theo đó doanh nghiệp sẽ cung cấp đào tạo để nâng cao kỹ năng cho nhân lực hiện có trong các lĩnh vực cần bổ sung nhân sự như: kỹ năng số, sự nhạy bén trong kinh doanh và kỹ năng xã hội. Một số doanh nghiệp đã bắt đầu sử dụng các dịch vụ quản lý vấn đề đào tạo để đáp ứng nhu cầu cấp thiết về chuyên môn sâu cũng như liên quan đến các công nghệ tiên tiến.

Ông Phó Đức Giang cho biết, nhiều công ty tại Việt Nam đang phải đối mặt với vấn đề tương tự. Làm sao để có được đội ngũ chuyên gia an ninh mạng với hiểu biết liên quan về vận hành doanh nghiệp vẫn là còn là thách thức.

"Chúng tôi tin rằng để có được đội ngũ CISO vững mạnh trong tương lai, việc nâng cao kỹ năng và đào tạo các kỹ sư an ninh mạng sẵn có là biện pháp tối ưu đối với các công ty trong nước. Những người có kiến thức về vận hành doanh nghiệp và khả năng xử lý các rủi ro không ngừng biến đổi về an ninh mạng sẽ giúp doanh nghiệp thích ứng và vượt qua những thay đổi nhanh chóng trong thời đại số", ông Phó Đức Giang chia sẻ.

Báo cáo của PwC cho rằng, các tổ chức an ninh mạng thế hệ mới sẽ có nhiệm vụ ba trong một: xây dựng niềm tin, xây dựng khả năng thích ứng, và tăng tốc đổi mới. Do đó, việc đầu tư vào công nghệ, quy trình và năng lực, và con người sẽ có vai trò quan trọng trong việc ứng phó với tội phạm an ninh mạng. Các kết quả đồng thời nhấn mạnh tầm quan trọng của các CISO trong vai trò lãnh đạo chuyển đổi trong doanh nghiệp.

Theo Lan Nguyễn