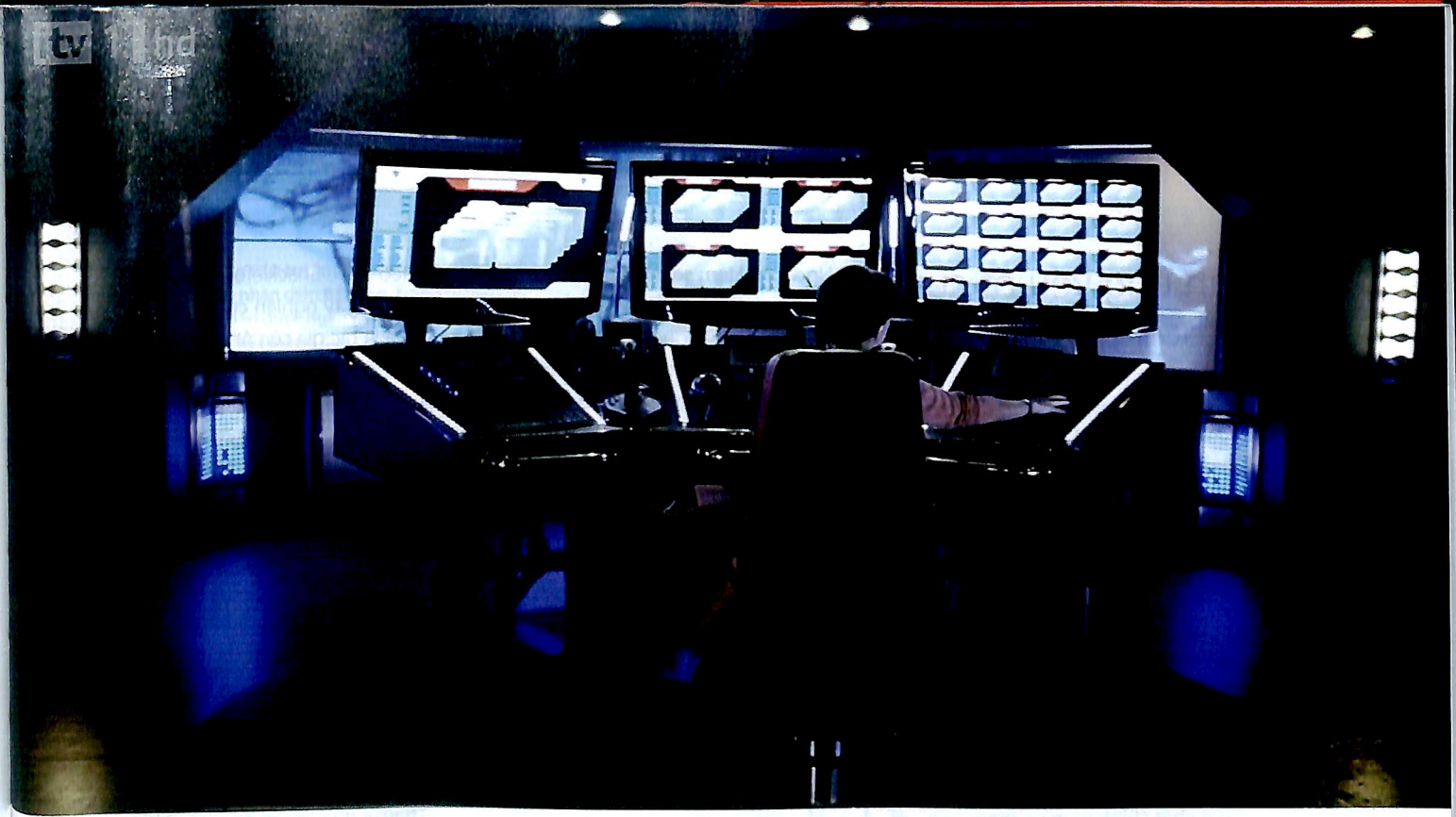


Hệ thống an ninh mạng thế hệ mới

Những chiếc máy thông minh có thể sử dụng hệ thống mạng của cảnh sát và lấp đầy khoảng trống mà nguồi lực cũng như trí tuệ con người đang bị hạn chế.

Con người rõ ràng không có khả năng giám sát hay xác định các mối đe doạ trên diện rộng và ngày càng trở nên phức tạp với các công cụ an ninh truyền thống. Chúng ta cần tăng cường khả năng của con người bằng cách kết hợp với các bộ máy thông minh. Tích hợp máy với con người là một trong số giải pháp mà các nhà khoa học đã nghĩ tới, tương tự như những gì OmniCorp đã làm trong bộ phim RoboCop (Cảnh sát người máy). Điều này không chỉ nâng cao khả năng của nhân viên an ninh mà còn giúp ngăn chặn mối đe dọa trước khi quá muộn.

Các công cụ hỗ trợ hiện nay được nhiều tổ chức sử dụng quá đơn giản và không hiệu quả. Nhìn lại các cuộc tấn công trước đây, chúng ta có thể thấy các tổ chức bị tin tặc tấn công trong một khoảng thời gian dài mà không được phát hiện, như công ty bảo hiểm y tế Premera Blue Cross từ năm 2014 đã bị rò rỉ dữ liệu y tế và thông tin tài chính của 11 triệu khách hàng, nhưng mãi đến tháng 3/2015 tổ chức này mới có thể xác minh rõ ràng. Xa hơn một chút nữa là cuộc tấn công nhắm vào Home Depot gây rò rỉ thông tin thẻ thanh toán của khoảng 56 triệu khách hàng tại gần như toàn bộ 2.200 cửa hàng trên toàn nước Mỹ. Một số cuộc tấn công lớn khác đáng chú ý như chuỗi nhà hàng P.F Chang hay hệ thống bán lẻ Target, Neiman Marcus và 6 chuỗi bán lẻ lớn khác của của Mỹ mất hàng chục triệu tài khoản thẻ tín dụng trong vòng 5 ngày.

Các tổ chức thường chỉ có phản ứng là quay lại nhìn về phía sau khi những cuộc tấn công đã xảy ra và cố gắng chỉ ra những tác nhân bên ngoài gây ra ảnh hưởng. Tìm kiếm các nguồn rò rỉ và khắc phục rõ ràng là việc quan trọng, tuy nhiên cách tiếp cận xử lý vấn đề này không thể bằng được việc phòng chống từ trước khi các cuộc tấn công diễn ra.

Những món lợi quá lớn từ việc xâm nhập các hệ thống như tiếp cận nhiều hơn các tập tin và dữ liệu quan trọng khiến cho các nhóm tin tặc ngày càng gia tăng. Nếu cho phép Premera, Sony, Target có khoản thời gian trước khi tấn công để dò xét và các lỗi trên hệ thống mạng thì cũng không thể chắc chắn được tin tặc có thể phát hiện một lỗ hổng nào khác hay không. Làm thế nào các tổ chức đảm bảo được việc không bị hacker ăn cắp dữ liệu? Hiện tại thì chưa thể có câu trả lời chắc chắn.

Phản ứng yếu ớt của hệ thống an ninh mạng

Cho đến gần đây, các tổ chức đã chỉ có một lựa chọn duy nhất trong việc phản ứng với các mối đe dọa là gia tăng bảo mật cho hệ thống của mình. Ví dụ như làm mới lại hệ thống, khóa chặt tường lửa và thiết lập mới các quy định cho IDS/IPS. Ngoài ra, tăng cường kiểm soát proxy hay tạo nên chính sách VPN trong môi trường làm việc. Tuy nhiên với cách làm này, các tổ chức sẽ bị đuối sức khi phải ứng phó liên tục với những sự cố được cảnh báo.

Thắt chặt chính sách và thêm vào lượng lớn các kịch bản nhằm đảm bảo tính an toàn thông tin chỉ làm cho mọi thứ khó khăn hơn đối với bộ phận an ninh khi lượng công việc bị dàn trải . Điều này có thể giúp phát hiện hàng ngàn lỗi trên hệ thống mỗi ngày, nhưng cũng khiến bộ phận an ninh không thể điều tra hết tất cả mọi hành vi. Khi những cuộc tấn công ở cấp độ cao gần đây đã chứng minh những cảnh báo dồn dập đã tạo ra nhiều kẽ hở để hacker xâm nhập, và một điều khác đáng chú ý là cho dù nắm bắt được các cuộc tấn công thì nhóm an ninh cũng chẳng thể làm gì.

Ngoài ra, kiểm soát chặt chẽ các quy tắc và thủ tục an ninh chỉ lãng phí thời gian của mọi người. Theo thiết kế, các chính sách thắt chặt sẽ hạn chế truy cập dữ liệu, và trong nhiều trường hợp dữ liệu đó là những gì nhân viên cần phải xử lý để phục vụ công việc của mình. Nhân viên và các phòng ban sẽ bắt đầu hỏi đến những công cụ và thông tin cần thiết, điều này khiến lãng phí thời gian cho họ và cho cả đội bảo mật khi phải đáp ứng tất cả mọi yêu cầu.

RoboCop có thể là một giải pháp điển hình

Máy thông minh có thể được sử dụng để giám sát các hệ thống mạng lớn, giúp lấp những khoảng trống khi nguồn lực sẵn có hạn chế và khả năng của trí tuệ con người chưa đủ đáp ứng. Cảnh sát RoboCop trong phim được áp dụng trên đường phố, còn trong những trường hợp chúng ta đang đề cập ở đây thì vũ khí mà nhân viên an ninh kỹ thuật số được trang bị là các thuật toán thống kê. Cụ thể hơn, số liệu thống kê có thể được sử dụng để phát hiện các hoạt động bất thường và xác định tính độc hại khi những điều đó xảy ra.

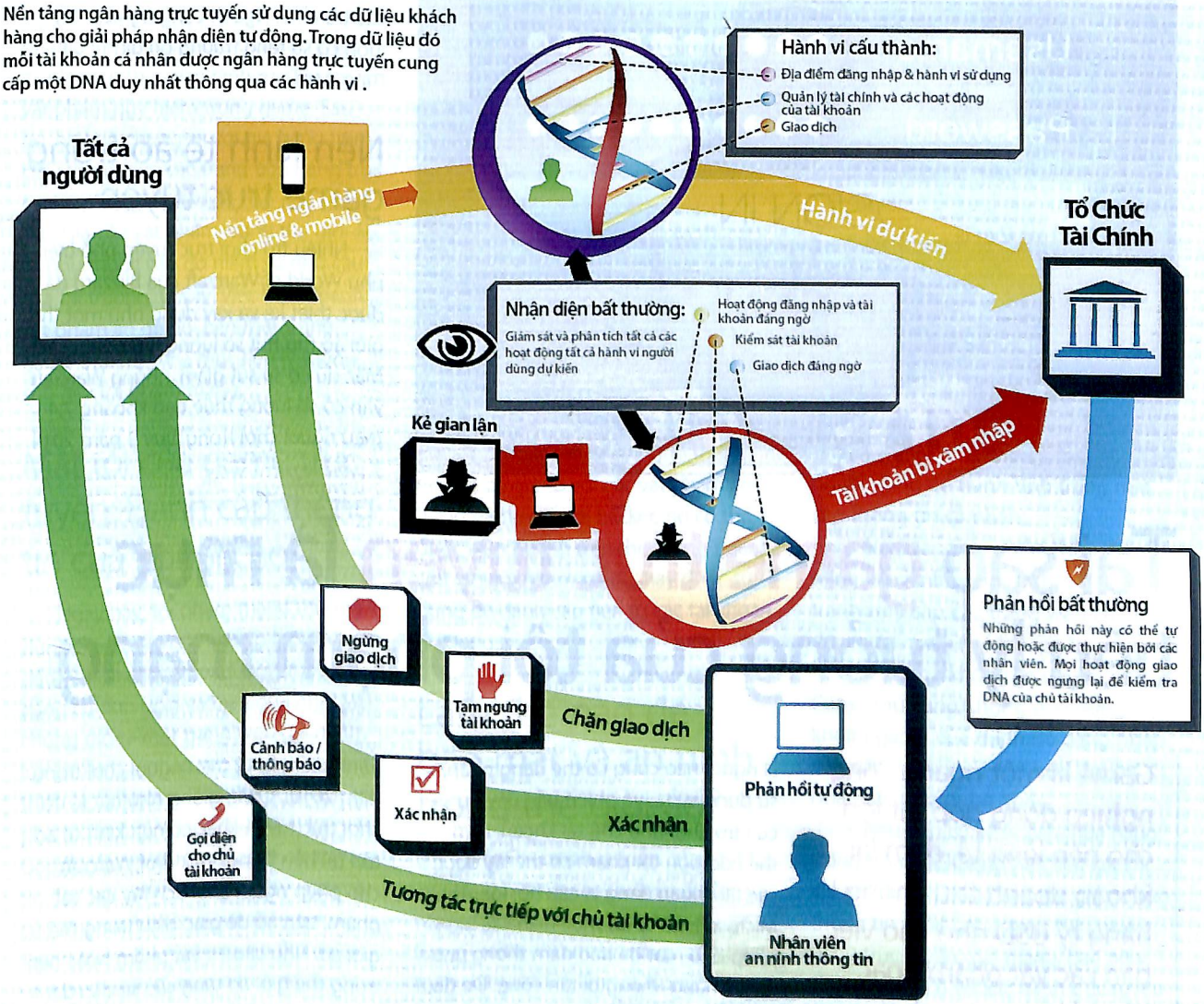
An ninh bảo mật cần một hệ thống mạnh mẽ hơn RoboCop

Theo Dave Shackleford, nhà phân tích tại công ty nghiên cứu bảo mật SANS và là tác giả của Analytics và Intelligence Survey 2014, một trong những thách thức lớn nhất của các tổ chức an ninh phải đối mặt là thiếu tầm nhìn vào những gì đang xảy ra trong môi trường công nghệ. Cuộc khảo sát diễn ra với 350 chuyên gia CNTT được hỏi tại sao họ gặp khó khăn trong việc xác định các mối đe dọa và phản hồi đầu tiên nhận được là khả năng của họ không thể hiểu và phát hiện ra những hành vi bất thường. Đây cũng là điều dễ hiểu, con người làm trong môi trường phức tạp khó có thể phân biệt hành vi bình thường hay bất thường.

Thay vì dựa vào con người để theo dõi những biểu đồ trên màn hình lớn, hoặc xác định các quy tắc và ngưỡng để phát cờ nếu ai đó vi phạm, máy thông minh có thể tìm ra và phân loại hành vi khi xử lý nhiều thông tin. Hơn thế nữa, máy với phần cứng mạnh có thể xử lý số lượng lớn thông tin mà các mạng tạo ra và thời gian thực thi sẽ đạt gần với thời gian thực. Máy có khả năng xử lý lên đến con số terabytes dữ liệu trong mỗi giây mà hệ thống mạng tạo ra, trong khi đó con người không thể xử lý quá 60 bit mỗi giây.

Bỏ qua yếu tố tốc độ và năng lực xử lý, một vấn đề lớn với cách thực thi truyền thống giám sát cho các vấn đề an ninh là nguyên tắc. Con người đặt quy tắc để cho máy để hành động và phải làm gì, những điều mà tốc độ xử lý và dung lượng không thể giải quyết. Trong khi các hệ thống giám sát dựa trên nguyên tắc, có thể rất phức tạp nhưng chúng ta vẫn đang được xây dựng trên một công thức cơ bản: "nếu điều này xảy ra, thì tiếp theo làm điều đó". Máy cung cấp dữ liệu tốt hơn và có cái nhìn sâu sắc về các hành vi để giúp con người dựa vào đó mà cải thiện tình hình an ninh.

Trong thế giới số, chúng ta không mong muốn nhận được những lời khuyên muộn trong việc bảo vệ, an toàn thông tin khi sự cố đã xảy ra. Đặc biệt là hiện tại chúng ta có



Nền tảng ngân hàng trực tuyến sử dụng các dữ liệu khách hàng cho giải pháp nhận diện tự động. Trong dữ liệu đó mỗi tài khoản cá nhân được ngân hàng trực tuyến cung cấp một DNA duy nhất thông qua các hành vi .

quyền đưa máy thông minh vào hoạt động để nhận ra các bất thường có thể được xảy ra ngay trước mắt. Máy móc có khả năng độc lập tìm hiểu và phát hiện hoạt động bất thường của hacker thông qua nhịp độ hoạt động dữ liệu.

Mô hình phát hiện bất thường của một hệ thống an ninh

Phát hiện bất thường là một trong những công nghệ đầu tiên mà máy học (machine learning) được đưa vào sử dụng để tăng cường cho hệ thống mạng và ứng dụng bảo mật. Đây không chỉ là thuật ngữ được sử dụng khá thường xuyên mà còn là một hình thức phân tích bảo mật tiên tiến. Một số yêu cầu cơ bản của hình thức này là khả năng triển khai dễ dàng để hoạt động liên tục, khả năng xử lý hàng đợi từ nhiều nguồn thông tin, và trong quá trình hoạt động với quy mô dữ liệu khổng lồ thì đưa ra các cảnh báo chính xác, độ trung thực cao nhằm giảm tải cho các đội an ninh.

Các nhà phân tích hàng đầu đồng ý rằng máy học sẽ là một phần không thể thiếu trong hệ thống an ninh mạng. Hồi tháng 11/2014, Gartner đã đưa ra báo cáo về hiệu suất trong việc sử dụng máy học để quản lý hệ thống, trong đó các chuyên gia khẳng định những thế hệ máy thông minh trong vòng 5 năm tới sẽ dần trở nên phổ biến và thời gian để máy tiến hóa sẽ sớm rút ngắn.

Máy học chắc chắn không phải là vũ khí tối thượng giúp con người giải quyết mọi thách thức an ninh, nhưng chắc chắn rằng những thiết bị này sẽ cung cấp dữ liệu tốt hơn để giúp con người đưa ra những quyết định chính xác. Và các tổ chức cũng nên ngừng đòi hỏi nhóm an ninh của mình làm những điều không thể mà hãy tiến thêm một bước mới với việc sử dụng máy thông minh.

THẠCH AN