2020

SỔ TAY

10 ĐIỀU CẦN BIẾT VỀ BẢO MẬT DỮ LIỆU
CÁC MẸO ĐỂ BẢO VỆ DỮ LIỆU
NHỮNG BƯỚC CƠ BẢN ĐỂ TỰ BẢO VỆ DỮ LIỆU

Chia sẻ trong khuôn khổ chiến dịch "Không bật mí những bí mật"

chonghack.com/khongbatminhungbimat

10 ĐIỀU CẦN BIẾT VỀ BẢO MẬT DỮ LIỆU

1. Bảo vệ dữ liệu và bảo mật dữ liệu khác nhau

Bảo vệ dữ liệu là bảo vệ dữ liệu chống lại các truy cập không được cho phép. Bảo mật dữ liệu là cho phép truy cập dữ liệu – ai được cho phép và ai cấp quyền cho phép. Một cách hiểu khác, bảo vệ dữ liệu là vấn đề kỹ thuật, trong khi bảo mật dữ liệu là vấn đề pháp lý.

2. Mọi nhân viên đều là một điểm yếu bảo mật dữ liệu đầy rủi ro

Nếu cho rằng bạn chỉ có một chuyên gia về an ninh mạng để đảm bảo an toàn dữ liệu của bạn, đây thực sự sẽ là thiếu sót lớn khi tất cả nhân viên đang làm việc với các dữ liệu nhạy cảm đều có thể bị khai thác và tấn công bởi hacker. Ví dụ, một nhân viên đang thao tác với các dữ liệu nhưng dùng Wifi công cộng hoặc Wifi không được bảo mật. Đây là một trong những mối nguy hiểm đáng lo ngại gắn với những nhân viên làm việc ngoài văn phòng (remote). Tội phạm có thể dễ dàng thiết lập một Wifi giả để điều hướng truy cập của người sử dụng, trực tiếp gửi mã độc (malware) vào máy tính của người sử dụng và theo dõi các hoạt động trực tiếp, bao gồm cả các hoạt động liên quan đến tổ chức của bạn. Tập huấn các nhân viên của tổ chức về an ninh mạng thông qua các buổi thảo luận và hội thảo là điều cần thiết trong thời đại nhu cầu sử dụng IT tăng cao đáng kể.

3. Lĩnh vực chăm sóc y tế thường dễ bị tấn công mã độc

Lĩnh vực chăm sóc y tế thường ít chú tâm hơn trong các vụ tấn công mạng ở trong lĩnh vực của họ. Vì những người trong lĩnh vực không thường xuyên phải xử lý các giao dịch tài chính trực tiếp, an ninh mạng và xa hơn là bảo mật dữ liệu không phải mối quan tâm hàng đầu của họ. Hơn 75% ngành chăm sóc y tế đã bị nhiễm mã độc chỉ tính riêng trong năm 2016, bao gồm các cơ sở điều trị và cơ quan bảo hiểm y tế. Dữ liệu cá nhân và nghiên cứu y tế luôn là mục tiêu chính của các hacker. Sau đó, các loại dữ liệu nhạy cảm này sẽ được bán trên chợ đen cho người trả giá cao nhất.

4. Lộ dữ liệu mất một thời gian dài để có thể phát hiện

Có thể phải mất đến 6 tháng để các công ty chuyên về công nghệ như Facebook, Equifax có thể nhận diện được một vụ việc lộ dữ liệu. Trong thời gian đó, hackers hoàn toàn có thể lọt khỏi vòng kiểm soát nhờ sử dụng mật khẩu, thẻ tín dụng, thông tin an sinh xã hội và các thông tin khác từ các dữ liệu bị đánh cắp. Ngay cả khi công ty phát hiện ra vụ việc lộ dữ liệu đang xảy ra, khó để lần theo chính xác những cá nhân nào nằm trong số những dữ liệu bị ảnh hưởng. Đây là lời cảnh tỉnh cho tất cả chúng ta cần phải đổi mật khẩu thường xuyên và chỉ chia sẻ thông tin cá nhân riêng tư qua mạng trong trường hợp cần thiết.

10 ĐIỀU CẦN BIẾT VỀ BẢO MẬT DỮ LIỆU

5. Phần mềm an ninh mạng trở thành công cụ cần có
Bất kỳ một tổ chức hoặc cá nhân nào ý thức được tầm quan trọng của dữ liệu đều nên đầu tư vào phần mềm an ninh mạng, thường là phần mềm chống mã độc. Những phần mềm chuyên dụng này được thiết kế để nhận biết và cách ly phần lớn những mối nguy về an ninh trước khi chúng chạy khắp cả hệ thống, tạo ra các thiệt hại lớn hơn.

6. Đã dễ dàng hơn để truy lùng các tên tội phạm mạng
Sự phát triển của các phần mềm nhận diện trong những năm gần đây là tương lai trong ngành chống lại tội phạm mạng, khi giờ đây người dùng có thể xác minh các cá nhân bằng cách sử dụng một hoặc nhiều phần thông tin. Vì vậy, nếu như bạn nghi ngờ một mail mới nhận được là rủi ro an ninh, bạn có thể kiểm tra với người gửi trước khi mở hoặc tải tài liệu được đính kèm.

7. Bảo mật mạng cũng rất quan trọng.
Hiện tại, mọi dữ liệu cá nhân và hoạt động trực tuyến: email, chuyển khoản Internet (e-banking), mua sắm trực tuyến, tìm kiếm thông tin, dữ liệu y tế, tài khoản ngân hàng, thông tin thẻ tín dụng được mở và công khai cho mọi người, vậy chúng ta thật sự “không có gì để giấu” không? Quyền riêng tư mạng rất quan trọng bởi vì nếu không có, khi chúng ta bắt đầu trực tuyến, mọi thông tin sẽ đều được công khai, và rủi ro chúng ta bị điều hướng, kiểm soát, đe doạ chắc chắn sẽ tăng cao.

8. Các quảng cáo hiểu chúng ta
Các nhà quảng cáo đang theo dõi các hoạt động trực tuyến của bạn thông qua các website, fanpage mà bạn theo dõi bằng cách dựa vào lịch sử Cookies và các thủ thuật khác. Về cơ bản, các hoạt động trực tuyến của bạn đều bị theo dõi và tạo nên một hồ sơ hoàn chỉnh và đầy đủ về thói quen sử dụng mạng của người dùng. Cách nhanh nhất để bảo đảm quyền riêng tư mạng là ngắt kết nối và xoá cookies bất kỳ khi nào bạn có thể.

9. Sử dụng lại các mật khẩu có thể khiến dữ liệu của bạn dễ bị hack hơn
Dùng đi dùng lại 1 mật khẩu trên nhiều thiết bị, trang web hoặc ứng dụng khác nhau có thể gây ra rủi ro cao vì hacker có thể lấy hết các tài khoản của bạn khi có quyền truy cập vào một trong số các tài khoản. Lời khuyên là các bạn nên sử dụng một ứng dụng để quản lý mật khẩu. Hơn nữa, bạn nên sử dụng bảo mật hai lớp để giảm thiểu rủi ro.

10. Sử dụng phiên bản cũ của các hệ điều hành khiến bạn dễ bị tấn công mạng hơn

Các mẹo để bảo vệ: Dữ liệu nào là nhạy cảm?

Theo quy định tại Khoản 8 Điều 2 Thông tư 31/2015/TT-NHNN Quy định về đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin trong hoạt động ngân hàng do Thống đốc Ngân hàng Nhà nước ban hành thì nội dung này được quy định như sau:
Dữ liệu nhạy cảm là dữ liệu có thông tin mật, thông tin lưu hành nội bộ của đơn vị hoặc do đơn vị quản lý, nếu lộ lọt ra ngoài sẽ gây ảnh hưởng xấu đến danh tiếng, tài chính và hoạt động của đơn vị.

Đối với GDPR (General Data Protection Regulation) – Luật Bảo vệ Dữ liệu Châu Âu
Dữ liệu nhạy cảm được quy định dưới hạng mục dữ liệu cá nhân đặc biệt trong GDPR. Định nghĩa dữ liệu cá nhân nhạy cảm là bất kỳ dữ liệu nào tiết lộ "Chủng tộc hoặc sắc tộc, tư tưởng chính trị, đức tin tôn giáo, quan niệm triết lý, thành viên công đoàn, và việc xử lý dữ liệu sinh thực và sinh trắc nhằm mục đích định danh hoặc dữ liệu liên quan đến sức khoẻ, tình trạng sinh dục, và xu hướng tính dục.
Việc xử lý và phân tích các dữ liệu nhạy cảm nói trên là hoàn toàn bị cấm bởi GDPR. Một số trường hợp ngoại lệ cho việc xử lý dữ liệu nhạy cảm cần phải có sự đồng thuận từ chủ thể (chủ thể nhận thức rõ ràng về mục tiêu khai thác, thời gian khai thác, đơn vị khai thác và đồng ý trong tình trạng có hiểu biết rõ ràng về vòng đời của dữ liệu được cung cấp), bảo vệ quyền lợi cá nhân, công tác y tế dự phòng và y tế nghiệp vụ, hoặc lợi ích chung. Xét trên những định nghĩa nêu trên, việc Facebook hoặc Google cùng các đối tác kinh doanh thu thập và xử lý các dữ liệu cá nhân có khả năng vi phạm GDPR rất cao.

Vòng đời của một dữ liệu nhạy cảm
Dữ liệu được tạo. Một nhân viên nhập dữ liệu nhạy cảm của khách hàng vào bảng tính Excel trên máy tính xách tay của mình. Ở giai đoạn này, bộ phận CNTT có thể chuẩn bị cho tình huống này bằng cách thiết lập các chính sách mã hóa cho cả tệp và máy tính xách tay để bảo vệ thông tin.

Dữ liệu nhạy cảm được phát hiện bằng cách quét dữ liệu khi truyền qua các thiết bị, ứng dụng và dịch vụ. Nhân viên lưu bảng tính của mình vào đám mây để chia sẻ với các thành viên trong nhóm. Khi anh ta tải tệp lên, máy quét sẽ phát hiện dữ liệu được cho là nhạy cảm, như số An sinh xã hội, dựa trên các chính sách được tạo bởi một nhóm CNTT hoặc bảo mật.

Các mẹo để bảo vệ: Dữ liệu nào là nhạy cảm?

Dữ liệu được phân loại và đánh nhãn để thể hiện mức độ nhạy cảm. Nhiều biện pháp khác nhau có thể được áp dụng cho dữ liệu dựa trên mức độ nhạy cảm. Ví dụ: nếu một tệp Excel của nhân viên chứa số ID nhân viên, tệp đó có thể được đánh nhãn Bí mật. Tuy nhiên, tệp này lại chứa Số an sinh xã hội nên sẽ được đánh nhãn Tuyệt mật.

Sau khi dữ liệu được đánh nhãn, chính sách bảo mật được tạo bởi nhóm CNTT hoặc bảo mật có thể được tự động áp dụng cho tệp. Các chính sách này xác định những biện pháp bảo vệ sẽ được áp dụng cho tệp: mã hóa, hạn chế quyền truy nhập, hình đánh dấu hoặc hình nền mờ, chính sách giữ hoặc xóa hoặc hành động bảo vệ rò rỉ dữ liệu như chặn người dùng chia sẻ tệp.

Nhân viên cần chia sẻ tệp với các liên hệ tại máy khách để họ có thể xem lại thông tin. Để làm điều này, anh ta sẽ gửi tệp qua email. Vì bộ phận CNTT đã đánh nhãn và thiết lập chính sách bảo mật, khi dữ liệu truyền đi, việc bảo vệ tệp sẽ được duy trì. Trong trường hợp này, lệnh hạn chế quyền truy nhập đã được đặt cho tệp, vì vậy chỉ những người cụ thể mới có thể mở tệp.

Ngoài ra, nhóm CNTT có thể theo dõi việc truy nhập và chia sẻ tệp, các cảnh báo hoặc email sẽ được gửi đi nếu phát hiện vi phạm hoặc mối đe dọa. Nếu nhân viên bỏ qua cảnh báo ngăn chặn mất dữ liệu (Data loss prevention - DLP) và cố tình gửi bảng tính cho người không có quyền truy nhập, bộ phận CNTT sẽ nhận được cảnh báo ngay lập tức để có thể nhanh chóng hành động.

Cuối cùng, theo thời gian, bảng tính sẽ phải đối mặt với việc hết hạn, lưu giữ hoặc xóa bỏ. Việc quản trị dữ liệu này là một khía cạnh quan trọng của bảo vệ thông tin tổng thể, bởi dữ liệu nhạy cảm tồn tại trong môi trường lâu hơn cần thiết thường sẽ tạo ra rủi ro không đáng có khi bị tìm ra và xâm phạm.

Các bước đơn giản để tự bảo vệ

1 MÃ HOÁ DỮ LIỆU

Ngày này, chúng ta đọc báo, mua thực phẩm hay thậm chí cả nộp thuế thông qua Internet. Tất cả những hoạt động trực tuyến đều tiềm ẩn nguy cơ về bảo mật thông tin. Mặc dù nghe về thuật ngữ "mã hoá" hàng ngày, nhưng vì e ngại phức tạp, nên nhiều người không chọn sử dụng phương pháp này. Thật ra, việc sử dụng các phần mềm mã hoá để bảo vệ dữ liệu trong máy tính và ổ cứng gắn ngoài một cách hiệu quả bây giờ khá dễ dàng.

2 SỬ DỤNG MẬT KHẨU MẠNH

Việc mã hoá dữ liệu sẽ trở nên vô giá trị nếu kẻ xâm nhập dễ dàng lần ra mật khẩu bảo vệ của bạn. Mật khẩu mạnh là mật khẩu dài với sự kết hợp giữa các chữ cái, chữ số và biểu tượng. Những công cụ trực tuyến miễn phí sau đây sẽ giúp bạn tạo một mật khẩu mạnh mẽ mà ngay cả phương thức tấn công cưỡng bức cũng khó có thể phá vỡ: PC Tools Random Password Generator, Good Password, Strong Password Generator, GRC Ultra High Security Password Generator.

3 XÁC MINH HAI BƯỚC

Dù cho đã mã hoá dữ liệu và có một mật khẩu mạnh, bạn vẫn có nguy cơ bị mất mật khẩu này khi truyền qua mạng không dây công cộng không an toàn. Để tự bảo vệ mình, bạn có thể sử dụng chế độ xác minh hai bước (hay chứng thực hai lớp), có nghĩa là ngoài mật khẩu, bạn cần một thông tin khác để đăng nhập vào trang website hay dịch vụ.
Google cung cấp dịch vụ xác thực hai lớp siêu bảo mật: ngay cả ai đó có được mật khẩu tài khoản Google của bạn, họ cũng không thể đăng nhập vì không biết mã 6 chữ số được tạo ra ngẫu nhiên mỗi 30 giây gửi đến trực tiếp điện thoại của bạn qua tin nhắn hoặc cuộc gọi thoại. Bên cạnh Google, nhiều dịch vụ phổ biến khác cũng vận hành cơ chế bảo mật này như Facebook, Dropbox, Microsoft, Paypal, v.v

4 SỬ DỤNG PHẦN MỀM DIỆT VIRUS

Các bước bảo mật trên có thể trở nên vô ích nếu virus hoặc malware (mã độc) đã xâm nhập trái phép vào hệ thống của bạn giúp tin tặc kiểm soát máy tính của bạn từ xa hoặc chuyển dữ liệu từ máy tính của bạn đến các máy chủ của chúng. Sử dụng các chương trình antivirus là điều vô cùng cần thiết cho mọi máy tính. Các giải pháp bảo mật của Symantec, Trend Micro, hay firewall của Palo Alto, Fire Eye là lựa chọn hoàn hảo dành cho bạn.

Do Liên minh Châu Âu tài trợ

OXFAM

IPS Institute for Policy Studies and Media Development

VIETNET-ICT

Tài liệu này được sản xuất với sự hỗ trợ của Liên minh Châu Âu (EU) và tổ chức Oxfam tại Việt Nam. Các ý kiến, phân tích và khuyến nghị trong tài liệu này do Ban tổ chức chiến dịch Không bật mí những bí mật chịu trách nhiệm, không nhất thiết phản ánh quan điểm chính thức của Liên minh Châu Âu và tổ chức Oxfam tại Việt Nam.