
Kingston
TECHNOLOGY
Bảo vệ dữ liệu và an ninh mạng trong bối cảnh hậu GDPR
#KingstonIsWithYou

Bảo vệ dữ liệu và an ninh mạng trong bối cảnh hậu GDPR

Lời nói đầu

Rất nhiều công ty và tổ chức đã làm việc tích cực – và tuyển dụng tích cực – để chuẩn bị cho GDPR. Có lẽ tổ chức của bạn cũng là một trong số đó. Nhưng đặc tính luôn biến đổi của các mối đe dọa trên mạng đồng nghĩa với việc bạn không thể dừng lại và nghỉ ngơi. Việc tuân thủ GDPR không phải là một việc làm hình thức mà là một khuôn khổ mà qua đó nhằm đánh giá nỗ lực bảo vệ dữ liệu và an ninh mạng của bạn. Không có chỗ dành cho sự thỏa hiệp.

Trong cuốn ebook ngắn này, chúng tôi tập hợp dữ liệu của một số nhà bình luận nhiều kinh nghiệm nhất về an ninh mạng tại Anh để thảo luận xem việc bảo vệ dữ liệu đã thay đổi như thế này kể từ lúc ban hành GDPR. Chúng tôi cũng nói đến việc cách thức các công ty đang đào tạo nhân viên của mình về sự cần thiết phải tuân thủ và thảo luận cách thức các phòng IT và nhà cung cấp công nghệ có thể bảo vệ tốt hơn hạ tầng IT và đào tạo người dùng cuối về những thách thức bảo mật đang nổi lên.

Bảo vệ dữ liệu và an ninh mạng trong bối cảnh hậu GDPR

Người đóng góp

Cuốn ebook ngắn này được năm chuyên gia về bảo vệ dữ liệu và an ninh mạng biên soạn.

Rob Allen
@Rob_A_kingston

Rob là Giám đốc Tiếp thị & Dịch vụ Kỹ thuật tại Kingston Technology và đã làm việc tại công ty từ năm 1996. Trong vai trò của mình, Rob phụ trách việc giám sát PR, truyền thông xã hội, tiếp thị kênh tại bộ phận truyền thông tiếp thị kỹ thuật số và sáng tạo cho tất cả các nhãn hiệu và sản phẩm Kingston.

Tara Taubman-Bassirian
@clarinette02

Tara có rất nhiều chức danh: luật sư, người ủng hộ, nhà hòa giải, nhà nghiên cứu, nhà tư vấn, diễn giả và tác giả. Với kiến thức chuyên môn vượt trội trong các lĩnh vực như quyền riêng tư, sở hữu trí tuệ và bảo vệ dữ liệu, cô đã đạt được danh tiếng tại một số khu vực trên thế giới, nổi bật nhất là ở Anh, Pháp và Hoa Kỳ.

Rafael Bloom
@rafibloom73

Rafael là Giám đốc của Salvatore ltd. Trong vai trò này, anh giúp các công ty quản lý các thách thức và cơ hội chiến lược, thương mại và thủ tục tạo ra do sự thay đổi về công nghệ và quản lý.

Miriam Brown
@Kingston_MBrown

Giám đốc Tiếp thị Chiến lược B2B tại Kingston Technology và đã làm việc tại công ty từ năm 1997. Trong vai trò của mình, Miriam phụ trách chiến lược, nội dung và các chiến dịch tiếp thị cho toàn bộ sản phẩm B2B của Kingston.

Sally Eaves
@sallyeaves

GS Sally Eaves đã được mô tả là người dẫn đường cho công nghệ có đạo đức'. Cô mang đến kinh nghiệm sâu sắc từ vai trò là Giám đốc điều hành và Giám đốc công nghệ, với tư cách là một giáo sư về công nghệ mới nổi và nhà tư vấn chiến lược toàn cầu. Sally là một diễn giả quốc tế đã giành được nhiều giải thưởng, tác giả, nhà nghiên cứu và người có ảnh hưởng chia sẻ về lãnh đạo tư duy độc đáo và xác thực.

Bảo vệ dữ liệu và an ninh mạng trong bối cảnh hậu GDPR

Mục lục

Phần 1 – Bảo vệ dữ liệu đã thay đổi thế nào kể từ GDPR?

Các công ty đã tiến một bước dài. Trong hai năm qua, đội ngũ pháp lý đã mở rộng, việc tuyển dụng Chuyên viên bảo vệ dữ liệu đã tăng vọt[1] và việc tham vấn với các chuyên gia về sự riêng tư dữ liệu đã tăng lên. Việc hoàn thành đánh giá tác động bảo vệ dữ liệu (DPIA) giờ đây đã trở nên quen thuộc với hàng ngàn tổ chức.

Nhưng vẫn còn một chặng đường dài.

Một trong những thách thức lớn nhất với GDPR là bạn không thể lơi lỏng những việc mình đang thực hiện. Trong hầu hết các tổ chức gần như mọi nhân viên đều có thể phá vỡ quy định bất cứ lúc nào. Vấn đề sẽ trầm trọng hơn trong các lĩnh vực mà lực lượng lao động bị quá tải hoặc có mức độ tự chủ cao như y tế, giáo dục và luật. Ví dụ như trong ngành luật, nhiều luật sư sẽ thản nhiên trao đổi tình tiết nhạy cảm của vụ án thông qua một tệp đính kèm đơn giản trong email. Các nhân viên y tế sẽ trao đổi dữ liệu của bệnh nhân hoặc kết quả chụp MRI từ những địa chỉ email không bảo mật. Trong các tổ chức có áp lực cao, chỉ cần thêm một chút sức ép lên danh sách việc cần làm sẽ khiến việc tuân thủ không còn được thực hiện nữa. Dường như năng suất đã chiến thắng quy định.

Điều này cần phải thay đổi.

Tiếp đến là vấn đề ý thức trong lĩnh vực từ thiện. Các tổ chức từ thiện thường nghĩ rằng họ được miễn trừ GDPR. Ngay cả khi họ hiểu rằng GDPR áp dụng cho mọi tổ chức tư, công và lĩnh vực thứ ba, thì cũng dễ hiểu khi họ ngần ngại dành một phần tiền từ mục đích của mình để đầu tư vào việc bảo vệ dữ liệu. Điều đó thật cao thượng nhưng cũng thật ngây thơ. Các khoản phạt tiềm tàng khi vi phạm GDPR lớn hơn rất nhiều so với khoản chi tiêu có thể được dành ra cho IT.

Kể từ năm 2016 nhu cầu đối với Viên chức bảo vệ dữ liệu (DPO) đã tăng vọt ở mức trên 700%.

Tara Taubman-Bassirian
@clarinette02

GDPR, Bảo vệ dữ liệu & Tư vấn IP

"Nhiều tổ chức thuộc lĩnh vực thứ ba nói rằng: 'GDPR không áp dụng đối với chúng tôi, chúng tôi chỉ là một tổ chức từ thiện.' Ngay cả đối với việc tuân thủ trên trang web, tôi cố gắng nói với họ rằng đây không phải là về dữ liệu mà bạn muốn thu thập, đây là về bên thứ ba mà bạn đang cho phép truy cập dữ liệu của khách truy cập của bạn."

1. Varonis: Một năm với GDPR: Những thống kê và thông tin cần biết www.varonis.com/blog/gdpr-effect-review/ [truy cập vào 26/11/2019]

Bảo vệ dữ liệu đã thay đổi thế nào kể từ GDPR?

Tinh giản dữ liệu là một xu thế đáng hoan nghênh

Chúng ta sống trong thời đại thu thập dữ liệu khủng khiếp. "The Big Four" (bốn công ty lớn gồm Google, Apple, Facebook và Amazon) nắm giữ những khối lượng dữ liệu khổng lồ về người tiêu dùng. Có thể nói rằng các tổ chức khác cũng học theo The Big Four và thu thập dữ liệu nhiều nhất có thể. Nhưng bạn càng mang theo nhiều dữ liệu, bạn càng có nguy cơ gặp rủi ro. Một trong những xu thế tích cực nhất kể từ lúc ban hành GDPR là sự chống lại việc thu thập dữ liệu quá mức. Các công ty thông minh áp dụng tinh thần tinh giản dữ liệu: nếu bạn không cần, đừng thu thập.

Tara Taubman-Bassirian
@clarinette02

GDPR, Bảo vệ dữ liệu & Tư vấn IP

"Tinh giản dữ liệu có lẽ là một trong những nguyên tắc hay nhất của GDPR. Mọi việc tạo ra một cơ sở dữ liệu đồng nghĩa với việc tạo ra rủi ro."

Rob Allen
@Rob_A_kingston

Giám đốc Tiếp thị & Dịch vụ Kỹ thuật, Kingston Technology

"Chúng tôi có những quy định nghiêm ngặt về xóa dữ liệu. Đúng vậy, những dữ liệu tối quan trọng với hoạt động kinh doanh phải được lưu trữ đúng cách. Nhưng còn mọi dữ liệu khác thì sao? Sau một năm, chúng sẽ biến mất. Lưu giữ chúng để làm gì cơ chứ?"

Những lợi ích không chỉ nằm trong việc hạn chế rủi ro. Hãy lấy ví dụ về tiếp thị. Nếu cơ sở dữ liệu tiếp thị của bạn không sạch, có thể bạn đang nắm giữ những dữ liệu lỗi thời. Khi cơ sở dữ liệu của bạn lên đến hàng chục nghìn người, và bạn tiến hành các chiến dịch tiếp thị qua email thường xuyên, chi phí sẽ tăng lên. Nó cũng bóp méo thống kê hiệu suất của chiến dịch.

Tinh giản dữ liệu cũng áp dụng với dữ liệu vật lý. Hãy cẩn thận với những gì bạn in ra (như bản quét hộ chiếu khách hàng); hãy cẩn thận với những gì bạn viết ra (như mật khẩu tài khoản). Và khi bạn thực sự cần nắm giữ bản sao vật lý của một thứ gì đó, hãy lưu trữ nó một cách an toàn. Núi giấy tờ trên bàn của bạn có thể trông quan trọng. Nhưng nó không hề an toàn.

Rafael Bloom
@rafibloom73

Giám đốc,
Salvatore Ltd

"Chúng tôi đang chứng kiến một cách suy nghĩ hoàn toàn khác biệt về sự tương tác giữa công nghệ và những gì một doanh nghiệp đang thực sự làm. Mức độ trưởng thành kỹ thuật số đó trong tầng lớp lãnh đạo doanh nghiệp cần phải xảy ra nhanh chóng."

Tác động của việc lộ thông tin: từ lãnh đạo doanh nghiệp đến người tiêu dùng

Bảo vệ dữ liệu là một khái niệm quản lý đã xuất hiện hàng thập kỷ nay. Nhưng những khoản phạt lớn cho đến nay đối với các công ty như Google[1], British Airways và chuỗi khách sạn Marriott[2] – và sự chú ý của truyền thông mà chúng tạo ra – đã khiến tầng lớp lãnh đạo doanh nghiệp phải chú ý đến. Điều này đã gây ra hiệu ứng nhỏ giọt.

1. Varonis: Một năm với GDPR: Những thống kê và thông tin cần biết www.varonis.com/blog/gdpr-effect-review/ [truy cập vào 26/11/2019]
2. The Guardian: Tiền phạt GDPR: khoản tiền 300 triệu bảng của BA và Marriott sẽ đi đâu? www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [truy cập vào 26/11/2019]

Bảo vệ dữ liệu đã thay đổi thế nào kể từ GDPR?

Tiếp tục...

Một động lực phía sau xu thế tiếp nhận việc bảo vệ dữ liệu mạnh mẽ là kinh doanh hợp tác. Ngày nay các doanh nghiệp tiến hành thẩm tra sâu rộng tính toàn vẹn bảo mật dữ liệu của một nhà cung cấp tiềm năng bởi vì họ không muốn chịu trách nhiệm cho các sự cố rò rỉ dữ liệu do liên quan.

Cũng có một mặt trái của việc ý thức thương mại cao hơn về GDPR: người tiêu dùng ý thức hơn về các quyền dữ liệu của mình. Và họ biết rằng nếu một công ty mất quyền kiểm soát dữ liệu của họ – lưu ý: không nhất thiết là phải xảy ra rò rỉ – họ sẽ được quyền bồi thường. Các doanh nghiệp phải luôn tập trung.

Sally Eaves
@sallyeaves

CEO và Giám đốc,
Sally Eaves Consultancy

"Bảo vệ dữ liệu đã trở thành một mệnh lệnh kinh doanh mà ở đó bạn có thể giành được hoặc đánh mất niềm tin."

Phần 2 – Các tổ chức đang đào tạo nhân viên như thế nào?

Đào tạo nhân viên: hai từ có khả năng gây phản ứng tiêu cực từ lực lượng lao động của bạn.

Thêm lý do để chắc chắn rằng việc đào tạo của bạn có sự hấp dẫn. Một lực lượng lao động được đào tạo sẽ ít có khả năng vi phạm thực hành tốt về bảo vệ dữ liệu. Và nếu xảy ra rò rỉ dữ liệu, Văn phòng Viên chức Thông tin (ICO) sẽ có cái nhìn thiện cảm hơn với bạn trong đánh giá của họ, nếu bạn có thể chứng minh rằng bạn đã nỗ lực để đào tạo nhân viên của mình về bảo mật dữ liệu.

Rafael Bloom
@rafibloom73

Giám đốc,
Salvatore

"Tôi muốn nghĩ đến dữ liệu như một phần trong chuỗi cung ứng mà ở đó nguồn gốc và toàn bộ vòng đời của dữ liệu cần được quản lý phù hợp. Hẳn nhiên có thể tập hợp nhóm của bạn vào trong một căn phòng trong nửa giờ và bảo họ phải làm gì, không xé bỏ tài liệu, hãy sử dụng một mật khẩu tốt. Chắc chắn bạn đã giảm được rủi ro với tổ chức. Nhưng sau đó liệu thực sự có một sự khác biệt rõ rệt nào không ngoài tác động nhỏ ban đầu đó khi bạn gần như ép buộc mọi người? Không."

Tuy nhiên vào tháng 4 năm 2019, Bộ trưởng Kỹ thuật số Margot James cho thấy rằng ba trong mười tổ chức tại Anh đã đào tạo nhân viên để xử lý với các mối đe dọa trên mạng[1]. Đã đến lúc cần nghiêm túc xem xét việc đào tạo.

Đây là việc tạo dựng văn hóa, không phải đạo tạo hình thức.

Đào tạo là để tạo ra những thay đổi thực sự về hành vi và văn hóa, không phải là để đối phó. Rất dễ mua được một gói đào tạo trực tuyến với một số câu hỏi đơn giản về bảo mật dữ liệu mà ai cũng có thể trả lời đúng. Nhưng điều đó liệu có thực sự giúp bảo vệ tổ chức của bạn không?

Hành vi bảo vệ dữ liệu hiệu quả có hai thành tố cơ bản. Trước tiên, đó là đào tạo thông minh, hấp dẫn và hướng đến những thách thức riêng biệt với tổ chức của bạn. Thứ hai, đó là nhận thức rằng GDPR là một vấn đề sâu sắc về văn hóa nơi làm việc có ảnh hưởng hàng ngày đến mọi nhân viên. Đó là về việc làm những điều đúng đắn với dữ liệu, ngay trong toàn bộ tổ chức. Hãy lấy ví dụ về nhân sự. Hãy nghĩ đến thông tin cá nhân của tất cả các ứng viên đang nằm trên máy chủ email.
Bảo vệ dữ liệu là trách nhiệm của tất cả mọi người.

1. CISO thông minh: Một năm sau, tác động của GDPR đối với bảo mật dữ liệu là gì? www.intelligentciso.com/2019/04/16/one-year-on-what-has-been-the-impact-of-gdpr-on-data-security/ [truy cập vào 26/11/2019]

Các tổ chức đang đào tạo nhân viên như thế nào?

Có một người phía sau dữ liệu

Trong phần đầu tiên, chúng tôi đã chỉ ra rằng người tiêu dùng đang trở nên ý thức hơn về quyền dữ liệu của họ. Một cách để định vị việc đào tạo bảo vệ dữ liệu là giúp đỡ nhân viên của bạn hiểu rằng luôn có một người phía sau dữ liệu. Hãy yêu cầu nhân viên của bạn suy nghĩ về mọi tổ chức mà họ đã cung cấp dữ liệu cho và họ sẽ nhận ra rằng bảo vệ dữ liệu chính là về quyền riêng tư cá nhân.

Hãy có một kế hoạch dự phòng

Sally Eaves
@sallyeaves

"Đào tạo liên tục cho nhân viên về bảo mật dữ liệu và quyền riêng tư là một mệnh lệnh kinh doanh. Điều này không được phép chỉ là một phiên đào tạo duy nhất, mỗi năm một lần mà phải là một trải nghiệm chủ động, tương tác và hấp dẫn để nó trở thành một phần trong trải nghiệm công việc hàng ngày. Nhân viên phải tham gia đối thoại vào việc những gì chúng ta muốn giảm thiểu, quản lý và bảo vệ."

Miriam Brown
@Kingston_MBrown

"Tôi nghĩ rằng sẽ rất thú vị khi bạn nói điều này trong quá trình đào tạo: 'chuyện gì xảy ra nếu đó là dữ liệu của bạn?' Nếu quản lý ngân hàng của tôi làm việc tại nhà trên chiếc laptop của anh và có thông tin nhạy cảm trên chiếc máy đó, tôi sẽ muốn nó nằm trên một chiếc ổ được mã hóa."

Rob Allen
@Rob_A_kingston

"Hãy coi dữ liệu như thể đó là của riêng bạn."

Phần 3 – Liệu phòng IT có thể bảo vệ các thiết bị tốt hơn không?

Làm việc từ xa là trạng thái bình thường mới

Nhiều khả năng nhân viên của bạn truy cập thế giới công việc của họ từ một vài thiết bị khác nhau, bao gồm các thiết bị cá nhân có thể dễ dàng bị bỏ quên trên tàu hoặc thất lạc trên taxi. Thách thức của bạn là tìm cách để giúp nhân viên làm việc hiệu quả mà không trở nên dễ bị tổn thương trước các rủi ro bảo mật và rò rỉ dữ liệu. Chỉ cần một người sơ suất là nỗ lực bảo vệ dữ liệu của bạn sẽ đổ xuống sông xuống biển hết.

Sally Eaves
@sallyeaves

CEO và Giám đốc,
Sally Eaves Consultancy

"Dữ liệu cần được bảo vệ khi di chuyển, lúc nghỉ và khi đang sử dụng – việc tối quan trọng là có một kế hoạch bảo mật, khôi phục và xóa bỏ dữ liệu toàn diện để chuẩn bị cho tất cả những tình huống này. Thu hút sự chú ý đến các khu vực rủi ro thường được đánh giá thấp có ý nghĩa đặc biệt quan trọng, ví dụ như ổ USB không mã hóa, sử dụng email để gửi các tệp đính kèm không mã hóa và các tính năng của trình duyệt web tiết lộ dữ liệu nhạy cảm của người dùng. Với rất nhiều thiết bị được kết nối và phương thức làm việc đang thay đổi, điều tối quan trọng là bảo đảm rằng dữ liệu lưu trữ trên điện thoại di động cũng an toàn như dữ liệu lưu trữ trên máy chủ công ty."

Xác thực hai yếu tố

Đối với một tổ chức thông thường, đến nay điều tốt nhất và dễ dàng nhất mà bạn có thể thực hiện là bảo vệ tham số mạng – và điều đó thực sự có thể chỉ đơn giản như việc sử dụng trình quản lý mật khẩu và xác thực hai yếu tố. Một ví dụ điển hình về xác thực hai yếu tố là khi một người dùng được yêu cầu cung cấp mật khẩu trên laptop và mã xác thực được gửi đến điện thoại di động của họ sau khi cung cấp thành công mật khẩu.

VPN và SSD/USB mã hóa

VPN ngày càng phổ biến với các doanh nghiệp vừa và nhỏ (SME). Nó đặc biệt quan trọng đối với nhân viên truy cập dữ liệu doanh nghiệp qua mạng Wi-Fi công khai. Nhưng các doanh nghiệp phải cẩn thận đừng đánh giá quá cao khả năng của VPN. Nó là một phần thay vì toàn bộ giải pháp. Khá thường xuyên các doanh nghiệp triển khai VPN chỉ để những nhân viên làm việc từ xa sử dụng máy tính xách tay mà không có biện pháp mã hóa phần cứng nào. Gần như tất cả mọi người đều lưu trữ các tập tin trên laptop của mình. Chuyện gì sẽ xảy ra nếu thiết bị bị xâm nhập, thất lạc hay mất cắp? USB và SSD mã hóa chỉ đắt hơn một chút so với các phiên bản tiêu chuẩn. Triển khai USB mã hóa và trang bị SSD mã hóa phần cứng cho máy tính xách tay của bạn là một bước tiến dài trong việc giải quyết những thách thức khi làm việc từ xa. Và nếu một thiết bị bị thất lạc hoặc mất cắp, bạn có thể tự tin rằng không một ai sẽ có quyền truy cập các tập tin mã hóa. Bạn thậm chí còn có thể phá hủy các USB đã mất từ xa.

"Tôi đã từng gặp một chuyên gia an ninh mạng cố gắng thuyết phục CEO của một công ty sử dụng xác thực hai yếu tố nhưng đã bị phản đối: 'Không chúng tôi sẽ không làm vậy, thêm một bước nữa phiền phức lắm, tôi không cần điều đó.' Không lâu sau họ trở thành nạn nhân của một vụ lừa đảo trị giá 40.000 bảng Anh."

Rafael Bloom
@rafibloom73

Giám đốc, Salvatore Ltd

"Cuối cùng phương thức tốt nhất để tăng cường ý thức bảo mật là mở đối thoại với nhân viên để tìm các chiến lược vừa an toàn vừa hiệu quả."

Rob Allen
@Rob_A_kingston

Giám đốc Tiếp thị & Dịch vụ Kỹ thuật, Kingston Technology

Liệu phòng IT có thể bảo vệ các thiết bị tốt hơn không?

Máy chủ riêng và MSP

Ngày càng nhiều các tổ chức lớn đang tiến đến việc sở hữu lại máy chủ tại chỗ của riêng mình. Điều này có nghĩa là họ có toàn quyền kiểm soát tài nguyên máy chủ của mình, không lưu trữ thứ gì trên đám mây truy cập công khai. Và còn có giải pháp máy chủ lai trong đó dữ liệu phi nhạy cảm vẫn nằm trên đám mây còn dữ liệu cá nhân nằm tại chỗ. Đối với SME và các tổ chức thuộc khu vực thứ ba, việc sở hữu máy chủ riêng có thể quá đắt đỏ. Và đó là nơi mà các nhà cung cấp dịch vụ quản lý và máy chủ riêng ảo xuất hiện. Giải pháp này tăng cường tập trung vào bảo mật mà không làm tăng đáng kể chi phí vận hành của bạn.

Tự động đánh dấu dữ liệu sắp hết hạn

Một trong những nguyên tắc của GDPR là sự cần thiết phải xóa dữ liệu cũ. Ví dụ như, một số loại dữ liệu cá nhân nhất định không được lưu giữ quá bảy năm. Điều gì sẽ xảy ra nếu bạn được tự động nhắc nhở khi dữ liệu chuẩn bị 'hết hạn'? Với cơ sở dữ liệu đúng, sẽ rất dễ để đội ngũ IT tạo ra một thao tác gửi một email được tạo ra tự động đến DPO khi sắp đến hạn chấm dứt lưu giữ dữ liệu.

Hợp tác với nhà cung cấp phù hợp

Khi nói đến bảo mật IT, có rất nhiều nhà sản xuất và nhà cung cấp. Hãy tìm hiểu. Điều quan trọng nhất là có một hệ thống được lắp đặt từ một nhà cung cấp tin cậy với kinh nghiệm cụ thể trong việc hỗ trợ các tổ chức trong ngành hoặc lĩnh vực của bạn. Bảo đảm rằng (các) nhà cung cấp mà bạn chọn không chỉ sở hữu công nghệ mà còn hiểu rõ những thách thức về việc áp dụng khi nói đến bảo mật dữ liệu.

Phần 4 – Các nhà cung cấp có thể cải thiện quy trình và hiểu biết như thế nào?

TLC cho DPO

Kể từ năm 2016, nhu cầu đối với Viên chức bảo vệ dữ liệu đã tăng vọt ở mức trên 700%.[1] Giờ đây có trên 500.000 DPO đang làm việc khắp châu Âu – con số này lớn hơn sáu lần so với dự đoán đưa ra vào năm 2017.[2] Đấy là trong khi tầm quan trọng của DPO thường bị bỏ sót và coi nhẹ.

Một DPO yêu cầu tầm nhìn đầy đủ về thực trạng bảo mật và sự riêng tư dữ liệu của công ty bạn. Đây là một công việc toàn thời gian. Nhưng ở một số công ty 'DPO' chỉ đơn giản là một chức danh được gán cho một nhân viên hiểu rõ công nghệ nhất. Họ chịu trách nhiệm đối với sự riêng tư dữ liệu của toàn bộ công ty, trong khi vẫn thực hiện những nhiệm vụ trong công việc hàng ngày của họ.

Thực tế là cần có một loạt các dịch vụ và công cụ chuyên nghiệp sẵn sàng để hỗ trợ kiểu DPO mới này. Ngay cả khi bạn có một DPO toàn thời gian, bảo mật dữ liệu thay đổi rất nhanh chóng và luôn có những thách thức đòi hỏi một ý kiến thứ hai. Hợp tác với một công ty tư vấn hoặc chuyên gia bên ngoài về bảo mật dữ liệu có thể là một bước tiến dài nhưng trước tiên bạn phải có mọi thứ gọn gàng nhất có thể trong nội bộ.

Minh bạch, dự phòng và gắn kết

Hạ tầng IT của bạn chỉ mạnh tương đương thành phần yếu nhất trong đó. Đó là lý do tại sao đối với một bổ sung mới vào hệ sinh thái IT của bạn, nhà cung cấp công nghệ cần hoàn toàn minh bạch về các mối đe dọa bảo mật tiềm tàng và đưa ra lời khuyên rõ ràng về cách sử dụng sản phẩm mới của bạn một cách bảo mật.

Tara Taubman-Bassirian
@clarinette02

GDPR, Bảo vệ dữ liệu & Tư vấn IP

"Tôi cố gắng giải thích với những người lắp đặt camera an ninh ở khắp mọi nơi rằng điều này không nhất thiết đồng nghĩa với bảo mật vì thường chúng được lắp đặt mà không có mật khẩu. Vì thế bạn có thể chỉ cần đăng nhập vào một trang web, ngồi và xem. Nó thực sự như là bảo với kẻ trộm rằng: 'hãy đến và xem khi tôi không ở đó!"

1. Varonis: Một năm với GDPR: Những thống kê và thông tin cần biết www.varonis.com/blog/gdpr-effect-review/ [truy cập vào 26/11/2019]
2. The Guardian: Tiền phạt GDPR: khoản tiền 300 triệu bảng của BA và Marriott sẽ đi đâu? www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [truy cập vào 26/11/2019]

Các nhà cung cấp có thể cải thiện quy trình và hiểu biết như thế nào?

Có vấn đề về dự phòng. Điều gì xảy ra khi một sản phẩm đến thời điểm kết thúc vòng đời hoặc cần cập nhật? Các nhà cung cấp công nghệ cần đưa ra lời khuyên dự phòng về các sản phẩm có thể tình cờ xâm phạm dữ liệu mà nó nắm giữ hoặc phơi bày điểm yếu bảo mật của hệ sinh thái IT rộng hơn. Hãy lấy ví dụ về máy chụp MRI. Nó có thể đi kèm với một ổ SSD mã hóa có dung lượng 4 terabyte để lưu trữ hình ảnh của bệnh nhân. Nhưng điều gì xảy ra khi hết dung lượng lưu trữ đó?

Các nhà cung cấp công nghệ và bản thân các tổ chức cũng phải hỗ trợ một môi trường gắn kết kỹ thuật số và gắn kết dữ liệu – cả bên trong tổ chức và khi làm việc với các nhà cung cấp và đối tác bên ngoài. Điều này đặc biệt quan trọng đối với các tổ chức đa phương diện, đa phòng ban và đa địa điểm như NHS.

Quét ngang

Công nghệ thay đổi rất nhanh, đôi khi nhanh hơn bảo mật. Với các công nghệ mới nổi – như thanh toán qua nhận dạng khuôn mặt ở Trung Quốc – đôi khi đó là chuyện các tổ chức chạy đua để đưa công nghệ ra thị trường trước khi xem xét các tác động về bảo mật và bảo vệ dữ liệu tiềm tàng. Sự phổ biến rộng rãi của mạng 5G sẽ xuất hiện trong một hoặc hai năm nữa trong đó điện toán biên và tháp dữ liệu phân tán sẽ trở thành hiện thực. Các nhà cung cấp công nghệ phải có khả năng giúp đỡ các tổ chức thu được lợi ích từ các công nghệ mới nổi một cách an toàn mà không hi sinh tính toàn vẹn dữ liệu hoặc bảo mật IT của riêng họ.

Miriam Brown
@Kingston_MBrown

Giám đốc Tiếp thị Chiến lược B2B tại Kingston Technology

"Chúng tôi đã bán rất nhiều sản phẩm cho NHS - nhưng có sự khác biệt rõ rệt từ chi nhánh này đến chi nhánh khác, khi chúng tôi hỏi họ đang có những chính sách và quy trình bảo vệ dữ liệu nào."

Sally Eaves
@sallyeaves

CEO và Giám đốc, Sally Eaves Consultancy

"Tôi tin rằng chúng ta sẽ bắt đầu thấy được sự thay đổi trong GDPR, thay vì giảm phiền phức của việc thực thi để tập trung vào tối ưu hóa các lợi ích, như tăng cường các quy trình IT, sao lưu và khôi phục, và cải thiện tính bảo mật, và sử dụng những điều này như là điểm khác biệt so với những công ty trong cùng ngành."

Tóm tắt

GDPR đã thay đổi doanh nghiệp theo hướng tốt hơn, khiến cho cả tầng lớp lãnh đạo và người tiêu dùng chú ý đến sự riêng tư dữ liệu và an ninh mạng. Tuy nhiên sự tuân thủ đòi hỏi chú ý thường xuyên đến bảo mật dữ liệu – ngày này qua ngày khác – trong suốt lực lượng lao động của bạn. Đặc tính thay đổi không ngừng của công nghệ và các mối đe dọa trên mạng đồng nghĩa với việc hạ tầng bảo mật tốt và đào tạo hiệu quả – nhờ hỗ trợ tư vấn hiệu quả về công nghệ và sự riêng tư dữ liệu - cũng tối quan trọng đối với hoạt động kinh doanh. Nhắc nhở nhân viên rằng luôn có một người phía sau dữ liệu có thể là một bước tiến dài đến việc đưa một văn hóa bảo vệ dữ liệu bên trong lực lượng lao động của bạn. Và thay đổi văn hóa có hiệu quả hơn nhiều so với những buổi đào tạo hình thức.

Giới thiệu Kingston

Với 32 năm kinh nghiệm, Kingston có kiến thức để xác định và giải quyết các thách thức khi làm việc từ xa – giúp lực lượng lao động của bạn có thể dễ dàng làm việc một cách an toàn từ bất cứ đâu, mà không làm tổn hại tổ chức của bạn.

#KingstonIsWithYou