TRUY CẬP DỮ LIỆU TRONG DỊCH VỤ NGHIÊN CỨU BẢO MẬT CỦA CƠ QUAN THỐNG KÊ QUỐC GIA: CHẾ ĐỘ CHỨNG NHẬN CHO KẾT NỐI TỪ XA

Tóm tắt:

Phù hợp với Đạo luật Kinh tế số GBR, 2019 ('Đạo luật'), Dịch vụ Nghiên cứu Bảo mật (Secure Research Service - SRS) của Cơ quan Thống kê Quốc gia (Office for National Statistics - ONS) đã tiến hành đánh giá chính sách về các điều kiện mà dữ liệu vi mô có thể được truy cập cho mục đích nghiên cứu vì lợi ích chung, sử dụng kết nối từ xa với dịch vụ dữ liệu SRS. SRS đã phát triển một chương trình chứng nhận mới để cho phép kết nối tổ chức từ xa, thay thế khung đặc biệt đã được sử dụng cho đến thời điểm này. Chương trình chứng nhận mới nâng cao tính an toàn của các thiết lập từ xa thông qua việc chia sẻ rủi ro và giám sát hành vi của nhà nghiên cứu với các tổ chức sử dụng họ. Chương trình chứng nhận cung cấp một đảm bảo bổ sung cho chủ sở hữu tài sản thông tin (IAO) và nâng cao khả năng của ONS / SRS để có được bộ dữ liệu nhạy cảm chính thức mới cho mục đích nghiên cứu.

1. Dịch vụ Nghiên cứu Bảo mật và Khung 5 an toàn

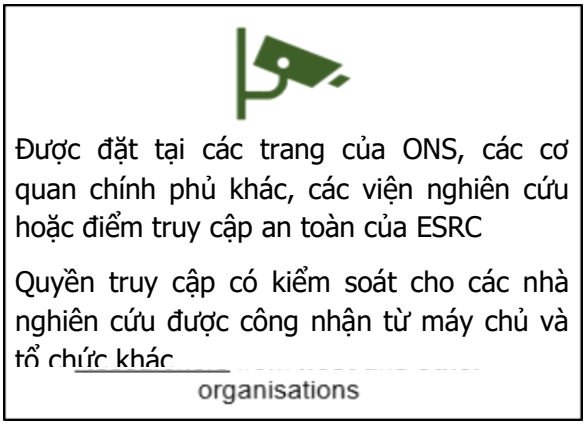
SRS hoạt động trong Khung 5 an toàn, một bộ nguyên tắc bảo vệ quyền truy cập vào dữ liệu nhạy cảm sẵn có để sử dụng bởi các thành viên được đào tạo và được công nhận của cộng đồng nghiên cứu (Nhà nghiên cứu được công nhận - AR). Phụ lục 1 đưa ra tóm tắt về Khung 5 an toàn.

Hình 1.1. Khung 5 an toàn

SRS là bộ xử lý dữ liệu được công nhận theo Đạo luật Kinh tế số của Vương quốc Anh 2017 (Đạo luật). Điều này có nghĩa là SRS không sở hữu dữ liệu được cung cấp thông qua dịch vụ và chủ sở hữu tài sản thông tin được xác định riêng trong Đạo luật. Điều quan trọng là chủ sở hữu tài sản thông tin phải hiểu rõ về cách hoạt động của thành phần cài đặt an toàn của khung vì họ có trách nhiệm chỉ định các điều kiện mà theo đó dữ liệu của họ có thể được truy cập (thông qua Thỏa thuận lưu ký dữ liệu của SRS).

Hiện tại, SRS hỗ trợ truy cập dữ liệu trong hai loại cài đặt an toàn: phòng an toàn và thông qua Kết nối tổ chức được đảm bảo (Assured Organisational Connectivity - AOC). Cả hai phương pháp đều hoạt động cùng với các 'két' khác trong khung để cung cấp dịch vụ nghiên cứu an toàn, nhưng có sự khác biệt quan trọng giữa chúng. Bài báo này là một hướng dẫn cho các bên liên quan bên ngoài quan tâm đến việc hiểu sơ đồ chứng nhận, bằng cách giải thích từng chi tiết hơn và đưa ra bản tóm tắt về các biện pháp kiểm soát an ninh được áp dụng.

2. Phòng an toàn



Hình 2.1 Các phòng an toàn là thiết lập an toàn

Phòng an toàn là các thiết lập an toàn có một số thiết bị đầu cuối cố định dành riêng cho nghiên cứu an toàn và được kiểm soát truy cập thông qua hệ thống đặt chỗ hoặc đặt phòng. Phòng an toàn thường sẽ được trang bị máy quay video hoặc các hệ thống giám sát khác. Các phòng an toàn thường mở cửa cho tất cả các nhà nghiên cứu được công nhận bất kể họ có phải là nhân viên toàn thời gian của tổ chức vận hành phòng an toàn hay không.

SRS duy trì một phòng an toàn tại mỗi địa điểm của nó ở Newport, Titchfield và London. Ngoài ra, có các phòng an toàn dành cho các nhà nghiên cứu được công nhận ở Belfast và Glasgow, và có một Mạng lưới Phòng an toàn đang phát triển tại các điểm nghiên cứu trên khắp Vương quốc Anh (chúng tôi có thể lấy thông tin chi tiết cập nhật về các địa điểm). ONS quan tâm đến việc thúc đẩy phạm vi tiếp cận theo khu vực và địa lý của các dịch vụ của mình cũng như đảm bảo quyền truy cập vào tất cả các phân nhóm cộng đồng nhà nghiên cứu và làm việc với các tổ chức nghiên cứu và cơ sở hạ tầng dữ liệu quan tâm đến việc lưu trữ các phòng an toàn. Phòng an toàn có các đặc điểm sau:

• Quyền truy cập được kiểm soát thông qua thao tác vuốt phím / bàn phím

• Thiết bị đầu cuối chuyên dụng không cần truy cập Internet

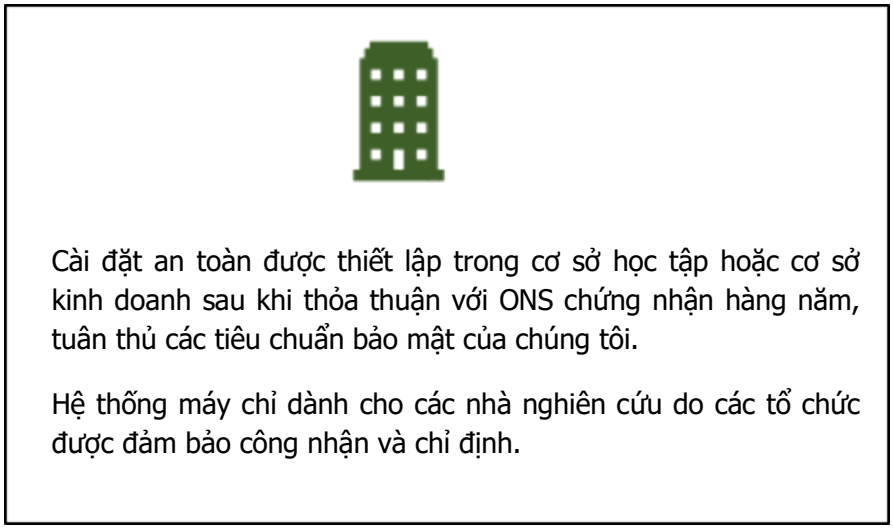
• Hệ thống đặt chỗ / đặt chỗ

• Camera và các biện pháp kiểm soát an ninh vật lý khác

Nghiên cứu và Đổi mới của Vương quốc Anh (UKRI), thông qua Hội đồng Nghiên cứu Kinh tế và Xã hội (ESRC), đang đầu tư vào việc cung cấp một mạng lưới các

phòng an toàn có chung những đặc điểm này thông qua chương trình 'safepod' (điểm truy cập an toàn) tại các trường đại học được chọn trên khắp đất nước. Điểm truy cập an toàn là những thùng loa dạng mô-đun được xây dựng có mục đích với tất cả các tính năng và kiểm soát an ninh của phòng an toàn. Chúng cung cấp một giải pháp thay thế rẻ và hiệu quả hơn để lắp đặt các phòng an toàn được xây dựng có mục đích và có thể được bố trí trong các cơ sở nghiên cứu hiện có như thư viện. Khi mạng safepod đã được ONS cài đặt và công nhận, mạng này sẽ cung cấp thêm quyền truy cập vào phòng an toàn cho SRS.

3. Các thỏa thuận của Kết nối Tổ chức được Đảm bảo (AOC)



Hình 3.1 Các thỏa thuận của AOC là cài đặt an toàn

Hệ thống Kết nối Tổ chức được Đảm bảo (AOC) đã được tạo cho các tổ chức đó, cho dù là cơ quan Chính phủ hoặc các cơ quan công quyền khác, các tổ chức học thuật, hoặc khu vực thứ ba / tổ chức thương mại hoạt động trong cộng đồng nghiên cứu, những người muốn truy cập SRS một cách an toàn từ cơ sở của họ. AOC hoạt động như một điểm đảm bảo cho SRS, chủ sở hữu tài sản thông tin và các bên liên quan khác. Nó nhằm chứng minh rằng các tổ chức lưu trữ cài đặt an toàn hiểu nghĩa vụ của họ, có thể đáp ứng các yêu cầu kỹ thuật về kết nối, có các biện pháp kiểm soát thích hợp và đồng ý duy trì các bản ghi hiện tại và chính xác về các kết nối và hoạt động.

Cách tiếp cận SRS đối với Kết nối Tổ chức được Đảm bảo công nhận rằng mọi cơ quan nghiên cứu hoặc tổ chức muốn kết nối với các dịch vụ của chúng tôi là khác nhau. Ví dụ, một số học viện (thường nhưng không phải luôn luôn) các học viện có thể có các khu học xá lớn, đa địa điểm, phần lớn mở cửa cho công chúng. Các tổ chức khác (ví dụ, nhiều cơ quan chính phủ) có kiểm soát truy cập chặt chẽ vào tất cả các khu vực trên trang web của họ và không cho phép khách truy cập không có người đi kèm. Chứng nhận có nghĩa là, bất kể loại hình tổ chức nào đang tìm kiếm kết nối, chủ sở hữu tài sản thông tin có thể yên tâm rằng các kết nối

tuân thủ các yêu cầu bảo mật vật lý và kỹ thuật nghiêm ngặt nhất.

Chứng nhận chứng minh rằng các tổ chức lưu trữ các cài đặt an toàn hiểu nghĩa vụ của họ, có thể đáp ứng các yêu cầu kỹ thuật về kết nối, có các biện pháp kiểm soát thích hợp và đồng ý duy trì các bản ghi hiện tại và chính xác về các kết nối và hoạt động. Điều đó cũng có nghĩa là các tổ chức sẽ giám sát các nhà nghiên cứu của họ và họ có các biện pháp trừng phạt thích hợp đối với bất kỳ hành vi vi phạm chính sách truy cập nào.

Để đảm bảo các tiêu chuẩn cao nhất về trách nhiệm giải trình, chỉ những nhà nghiên cứu có hợp đồng toàn thời gian hoặc toàn thời gian tương đương mới có thể đăng ký tham gia và chỉ thông qua tổ chức của họ. Nếu các nhà nghiên cứu được công nhận hoặc được phê duyệt không có hợp đồng với một tổ chức (ví dụ: họ là sinh viên trả phí hoặc cố vấn hoặc nhà tư vấn bên ngoài) thì họ sẽ cần truy cập SRS thông qua Phòng an toàn.

Các hiệp định AOC được ký kết trong thời hạn năm năm. Là một phần của thỏa thuận đó, các tổ chức muốn thiết lập các thiết lập an toàn đồng ý duy trì:

- Đăng ký cập nhật của các máy sẽ được kết nối với SRS. Họ cần cung cấp địa chỉ MAC của từng máy được kết nối, tên máy khách và địa chỉ IP nguồn (có thể được cấp quyền từ bỏ điều khoản này theo yêu cầu). Tất cả các máy cần thuộc sở hữu hoàn toàn của tổ chức và không thể yêu cầu kết nối cho bất kỳ máy hoặc thiết bị cá nhân nào.

- Một đăng ký cập nhật vị trí của từng máy được kết nối bao gồm cả địa chỉ IP. Đăng ký này phải bao gồm mô tả chính xác các điều khiển truy cập vật lý và kỹ thuật đối với mỗi máy. Khi máy được đặt trong không gian có thể được truy cập bởi những người không phải là các nhà nghiên cứu được công nhận có tên trong một dự án, sẽ cần phải giải thích về cách máy (và dữ liệu và đầu ra) sẽ được bảo mật (ví dụ: yêu cầu vật lý mô tả về không gian và cách thức ra vào được giám sát, và việc sử dụng các màn hình riêng tư, ngăn bàn, v.v. nơi các điều khiển vật lý khác không hạn chế quyền truy cập vào các máy được kết nối).

- Một đăng ký cập nhật các tài khoản cho các nhà nghiên cứu được công nhận sẽ yêu cầu quyền truy cập vào SRS và một dấu hiệu về những máy mà họ sẽ được tổ chức cho phép sử dụng. Mỗi nhà nghiên cứu yêu cầu kết nối phải ký vào một biểu mẫu Đăng ký Đảm bảo cho Nhà nghiên cứu được Công nhận, được cơ quan có trách nhiệm trong tổ chức của họ chỉ định và chứng thực cho sự hiểu biết của họ về các yêu cầu và nghĩa vụ kết nối.

4. Chứng nhận AOC

Chứng nhận diễn ra hàng năm và cung cấp một đảm bảo chắc chắn cho chủ sở hữu tài sản thông tin rằng các cài đặt an toàn của tổ chức tiếp tục hoạt động theo các tiêu chuẩn bảo mật được yêu cầu và tất cả hồ sơ và đăng ký của máy móc, cài đặt và người dùng được ủy quyền đều được cập nhật và chính xác. Khi các yêu cầu chứng nhận không được đáp ứng, kết nối sẽ bị tạm dừng cho đến khi ONS hài lòng rằng hành động khắc phục thích hợp đã được thực hiện. Trong trường hợp thiếu sót lặp đi lặp lại trong việc đáp ứng các yêu cầu

chứng nhận, các thỏa thuận sẽ bị chấm dứt.

Để duy trì các tổ chức chứng nhận cần phải:

• Đảm bảo rằng tất cả các đăng ký là hiện tại và cập nhật.

• Thông báo cho SRS về bất kỳ thay đổi nào đối với chứng nhận hiện tại (ví dụ: thêm máy móc hoặc địa điểm).

• Cung cấp quyền truy cập vào các đăng ký đó cho SRS, nếu được yêu cầu, trong vòng 48 giờ (2 ngày làm việc).

• Cho phép nhóm SRS kiểm tra địa điểm, nếu được yêu cầu, trong vòng năm ngày làm việc kể từ ngày yêu cầu.

• Thể hiện sự tuân thủ liên tục với tất cả các khía cạnh của thỏa thuận Kết nối Tổ chức được Đảm bảo.

5. Điều gì bị cấm trong Kết nối tổ chức được đảm bảo

Mục đích rõ ràng của chương trình chứng nhận AOC là cung cấp cho nhóm Bảo mật SRS và chủ sở hữu tài sản thông tin sự yên tâm rằng các nhà nghiên cứu được công nhận đang truy cập dữ liệu theo các tiêu chuẩn bảo mật cao nhất phù hợp với khung 5 An toàn. Chương trình AOC đặc biệt loại trừ một số hình thức kết nối. Cụ thể, chính sách nghiêm cấm:

• Việc sử dụng bất kỳ máy hoặc thiết bị cá nhân nào để kết nối với SRS.

• Việc sử dụng mạng không dây để kết nối với SRS (sự từ bỏ điều khoản này có thể được cấp theo yêu cầu, khi có thể chứng minh một cách thỏa đáng rằng mạng đạt được hoặc vượt quá các tiêu chuẩn bảo mật của mạng GovWiFi và / hoặc tiêu chuẩn an ninh mạng tối thiểu của Chính phủ và cho rằng không có giải pháp thay thế có dây thỏa đáng).

• Việc sử dụng mạng riêng ảo (Virtual Private Network – VPN) để kết nối với SRS (có thể từ bỏ điều khoản này khi VPN trong toàn tổ chức được ủy quyền như một phần của các biện pháp kiểm soát bảo mật của tổ chức đó. Thông thường, điều khoản này sẽ chỉ áp dụng cho các cơ quan của Chính phủ và các Cơ quan Nghiên cứu chuyên ngành, và sẽ cần được nhóm Bảo mật SRS xác minh là đáp ứng các tiêu chuẩn bảo mật VPN tuân thủ ONS).

• Thiết lập quyền truy cập vào SRS đối với bất kỳ máy nào đặt trong không gian công cộng (tức là máy không có kiểm soát vật lý hoặc giám sát việc truy cập). Máy tính xách tay không được sử dụng để kết nối ở bất kỳ vị trí nào khác với vị trí mà chúng được phê duyệt và chỉ định trong đăng ký do các tổ chức duy trì như một phần của chứng nhận.

Do đó, theo chương trình AOC, máy tính xách tay sẽ cần được kết nối qua ethernet trừ khi các điều kiện của chính sách miễn trừ có thể được chứng minh đầy đủ và tất cả các yêu cầu về vị trí và quyền truy cập trong chính sách này đã được đáp ứng một cách thỏa đáng (thường thì điều này sẽ chỉ áp dụng cho các cơ quan của Chính phủ).

6. Tóm tắt về Trách nhiệm / Kiểm soát An ninh

Các tính năng chính của các biện pháp kiểm soát an ninh và trách nhiệm duy trì sự an toàn của cài đặt truy cập từ xa được cung cấp trong Hình 6.1 dưới đây:

Kiểm soát an ninh		Phòng an toàn			Kết nối tổ chức được đảm bảo
		phòng an toàn của ONS	Phòng an toàn của OGD/máy chủ tổ chức	Điểm truy cập an toàn ESRC	
Bảo mật vật lý	Phòng/văn phòng an toàn	·	·	·	·
	Màn hình không bị bỏ qua bởi những người không phải là nhà nghiên cứu	·	·	·	·
	Giám sát an ninh (vd: CCTV)	·	·	·	·
SRS có thể được truy cập từ đâu?	Phòng thỏa thuận cụ thể	·	·	·	·
	Không gian thích hợp trong văn phòng đã thỏa thuận	·	·	·	·
	Ơ nhà/nơi công cộng	·	·	·	·
Đối tượng nào được truy cập vào SRS?	Các nhà nghiên cứu được công nhận	·	·	·	·
Dữ liệu nào có thể truy cập được?	Dữ liệu được chủ sở hữu dữ liệu phê duyệt rõ ràng	·	·	·	·
Bảo mật kỹ thuật số	Giám sát bảo vệ thời gian thực cho hoạt động đáng ngờ	·	·	·	·
	Ghi lại thao tác phím của tất cả các hoạt động nội bộ	·	·	·	·

Trách nhiệm kiểm soát	
	ONS được kiểm soát và đảm bảo
	OGD/Tổ chức được kiểm soát và đảm bảo
	ESRC và máy chủ Safepod được kiểm soát và đảm bảo
	Tổ chức nghiên cứu cam kết bằng văn bản
	Nhà nghiên cứu cam kết bằng văn bản

Hình 6.1 Tóm tắt các kiểm soát an ninh và trách nhiệm

Phụ lục 1: Khung 5 an toàn

Các biện pháp bảo vệ SRS truy cập và sử dụng dữ liệu thông qua Khung 5 an toàn:

Người an toàn

Các nhà nghiên cứu phải chứng minh sự hiểu biết về nghiên cứu và thống kê thông qua bằng cấp phù hợp hoặc thông qua kinh nghiệm làm việc có liên quan. Họ cũng phải hoàn thành khóa đào tạo được đánh giá. Sau khi các yêu cầu này được đáp ứng, một nhà nghiên cứu sẽ được coi là nhà nghiên cứu được công nhận theo Đạo luật Kinh tế số (DEA) và sẽ được phép sử dụng SRS trong khoảng thời gian 5 năm.

Dự án an toàn

Mỗi khi một nhà nghiên cứu được công nhận muốn thực hiện một dự án trong SRS thì nó phải được sự chấp thuận của Ban công nhận nghiên cứu độc lập giữa các chính phủ (RAP). RAP sẽ xem xét liệu dự án có khả thi, hợp pháp, đạo đức và vì lợi ích cộng đồng hay không trước khi phê duyệt.

Trước khi xem xét một đề xuất, phải có sự đồng ý về nguyên tắc của chủ sở hữu dữ liệu để dữ liệu của họ được sử dụng. Chủ sở hữu tài sản thông tin có thể đánh giá tính khả thi của một dự án yêu cầu sử dụng dữ liệu của họ hoặc giao trách nhiệm này cho Nhóm hỗ trợ thống kê SRS. Sau khi dự án được coi là khả thi và có thỏa thuận sử dụng dữ liệu được yêu cầu, nhóm Hỗ trợ thống kê sẽ xem xét đơn đăng ký dự án, bao gồm cả bằng chứng về sự chấp thuận về đạo đức, để đảm bảo rằng nó đã sẵn sàng để được đệ trình cho RAP.

Dữ liệu an toàn

Để đảm bảo rằng các nhà nghiên cứu không tìm hiểu bất cứ điều gì về các cá nhân hoặc doanh nghiệp trong khi thực hiện nghiên cứu của họ, tất cả dữ liệu có sẵn sẽ được loại bỏ nhận dạng bằng cách xóa số nhận dạng cá nhân. Chủ sở hữu tài sản thông tin cũng có thể muốn xem xét những biến nào khác trong nguồn dữ liệu có thể dẫn đến việc xác định lại gián tiếp.

Thiết lập an toàn

Khi một dự án đã được phê duyệt, các nhà nghiên cứu được công nhận sẽ được cung cấp quyền truy cập vào dữ liệu đã được xác định trong các phòng an toàn hoặc thông qua Kết nối Tổ chức được Đảm bảo.

Đầu ra an toàn

Khi một nhà nghiên cứu đã hoàn thành phân tích của họ, họ có thể yêu cầu đưa các kết quả tổng hợp không tiết lộ ra ngoài môi trường và sử dụng trong các báo cáo. Để đảm bảo tính bảo mật của các đối tượng dữ liệu được duy trì, hai người kiểm tra độc lập kết quả đầu ra để đảm bảo chúng đáp ứng các tiêu chuẩn bảo mật mà ONS áp dụng cho tất cả các đầu ra được công bố dưới dạng Thống kê chính thức. SRS hoạt động ngưỡng 10 cho hầu hết các nguồn dữ liệu mà họ nắm giữ. Tuy nhiên, chủ sở hữu nội dung thông tin có thể đặt mức ngưỡng cho dữ liệu của họ. Ví dụ: HMRC có xu hướng hoạt động ngưỡng 30.

Anh Tuấn (dịch)

Nguồn: https://unece.org/fileadmin/DAM/stats/documents/ece/ces/ge.46/2019/mtg1/SDC2019_S1_GBR_Engeli_AD.pdf