Australian Aid

BỘ LAO ĐỘNG - THƯƠNG BINH VÀ XÃ HỘI
TỔNG CỤC GIÁO DỤC NGHỀ NGHIỆP
DIRECTORATE OF VOCATIONAL EDUCATION AND TRAINING

Xu hướng mới về an ninh mạng

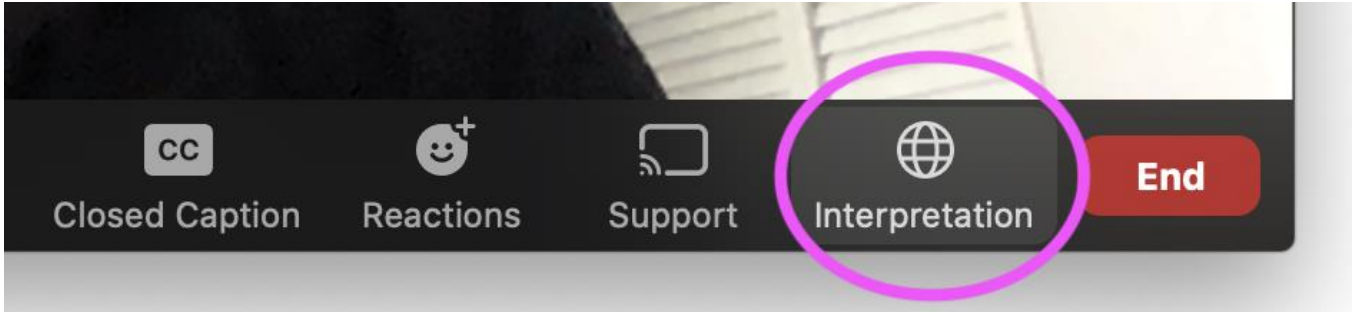
Hội thảo trực tuyến thứ 2

Thứ bảy, ngày 26/8/2023

AUS4SKILLS

RMIT UNIVERSITY

Lưu ý chọn đúng kênh phiên dịch trên Zoom



Australian Aid

BỘ LAO ĐỘNG - THƯƠNG BINH VÀ XÃ HỘI
TỔNG CỤC GIÁO DỤC NGHỀ NGHIỆP
DIRECTORATE OF VOCATIONAL EDUCATION AND TRAINING

Chương trình Hội thảo trực tuyến

Bắt đầu	Kết thúc	Thời gian	Tiêu đề phiên	Giảng viên
09:00	09:15	15	Giới thiệu về hội thảo trực tuyến	Michael Barton
09:15	09:40	25	Các mối đe dọa an ninh mạng + Hỏi đáp	Michael Barton
09:40	10:00	20	Thảo luận về các mối đe dọa tại Việt Nam	Michael Barton
10:00	10:30	30	Xây dựng chính sách an ninh mạng + Hỏi đáp	Michael Barton
10:30	10:50	20	Bảo mật dựa trên nền tảng đám mây/ kế hoạch + Hỏi đáp	Michael Barton
10:50	11:30	40	Mô phỏng các công cụ phòng chống tấn công an ninh mạng của RMIT	Michael Barton
11:30	11:50	20	Diễn giả khách mời từ doanh nghiệp	Nguyễn Quốc Cường
11:50	12:00	10	Kết luận và Kết thúc	Michael Barton

AUS4SKILLS

RMIT UNIVERSITY

GIÁO DỤC NHÂN VIÊN VÀ NGƯỜI DÙNG VỀ RỦI RO VÀ MỐI NGUY

Bằng cách đánh giá doanh nghiệp của bạn đang sử dụng CNTT như thế nào, bạn có thể:

- hiểu và xác định được loại rủi ro CNTT
- hiểu tác động của rủi ro đối với doanh nghiệp của bạn
- quản lý rủi ro bằng cách sử dụng chính sách, quy trình hiện có
- tiến hành đào tạo nhân viên thường xuyên để giảm thiểu rủi ro từ các mối đe dọa tiềm ẩn.

1. CÁC CHỦ ĐỀ CHÍNH TRONG ĐÀO TẠO NHÂN VIÊN

- **Chủ đề đào tạo phải phù hợp với chính sách bảo mật người dùng cuối của bạn. Các chủ đề chính, quan trọng với nhân viên bao gồm:**
- Lựa chọn mật khẩu mạnh
- Tránh nhấp vào liên kết hoặc mở tệp đính kèm trong email đáng ngờ hay email rác
- Phát hiện email giả mạo, lừa đảo
- Không bao giờ trả lời email yêu cầu cung cấp thông tin cá nhân, tài chính và mật khẩu
- Địa điểm và cách thức lưu trữ thông tin nhạy cảm
- Tránh sử dụng lại mật khẩu hoặc chia sẻ tài khoản người dùng không an toàn
- Đảm bảo an toàn cho thiết bị
- Phản hồi với sự cố bảo mật hoặc rò rỉ dữ liệu thực tế hoặc đáng ngờ.

2. CHÍNH SÁCH AN NINH MẠNG

- **Xây dựng chính sách an ninh mạng dành cho nhân viên, kết hợp với hoạt động đào tạo, có thể tăng cường bảo vệ cho hệ thống máy tính tại nơi làm việc của bạn hơn bất kỳ phần mềm đơn lẻ nào.**
- **Chính sách nên hướng dẫn nhân viên và tình nguyện viên sử dụng phù hợp internet và các công nghệ truyền thông khác, bao gồm các chủ đề như:**
  - mục đích sử dụng email và internet được chấp nhận
  - cách thức xử lý dữ liệu nhạy cảm
  - đảm bảo thiết bị an toàn
  - cách thức sử dụng internet an toàn
  - biện pháp cần thực hiện khi làm việc ngoài nơi làm việc chính thức.
  - Bạn nên giải thích chính sách cho nhân viên mới và hướng dẫn họ cách sử dụng công nghệ an toàn.

XÂY DỰNG CHÍNH SÁCH AN NINH MẠNG

- Nếu chưa có chính sách an ninh mạng, doanh nghiệp của bạn dễ trở thành đối tượng bị tấn công mạng.
- Xây dựng chính sách an ninh mạng để bảo vệ doanh nghiệp và lập kế hoạch biện pháp phản hồi nếu xảy ra sự cố.

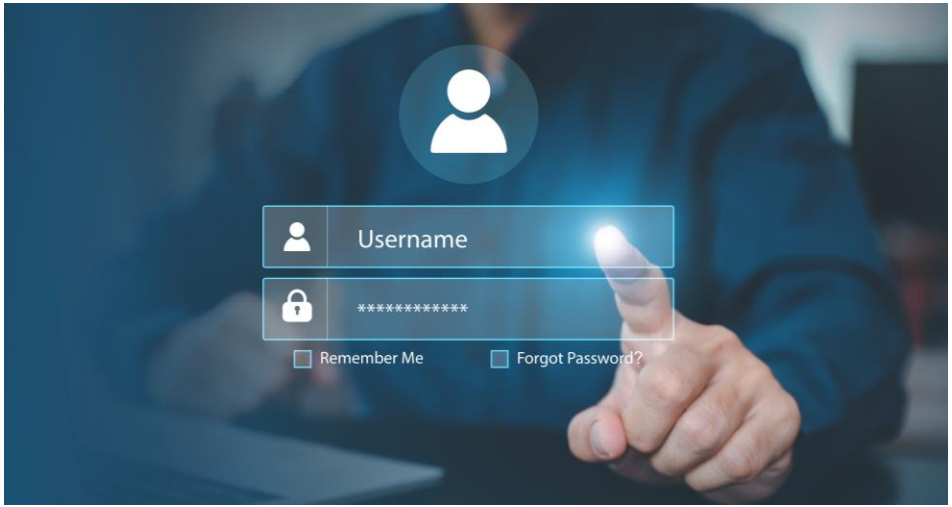
CHÍNH SÁCH AN NINH MẠNG LÀ GÌ?

- tài sản công nghệ và thông tin mà bạn mong muốn bảo vệ
- mối đe dọa đối với những tài sản đó
- quy tắc và biện pháp kiểm soát để bảo vệ tài sản và doanh nghiệp của bạn
- loại thông tin kinh doanh có thể được chia sẻ và chia sẻ ở đâu
- mục đích sử dụng thiết bị và nội dung trực tuyến phù hợp
- xử lý và lưu trữ dữ liệu nhạy cảm

Khi xây dựng chính sách an ninh mạng, lưu ý các bước sau…

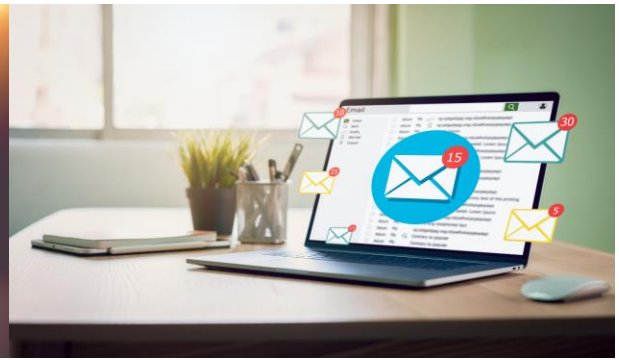
1. XÁC ĐỊNH YÊU CẦU MẬT KHẨU

- **Chính sách an ninh mạng cần làm rõ:**
- yêu cầu về cụm mật khẩu mạnh
- cách thức lưu trữ cụm mật khẩu chính xác
- tần suất cập nhật cụm mật khẩu
- tầm quan trọng của việc lập cụm mật khẩu riêng biệt cho các lần đăng nhập khác nhau



2. XÁC ĐỊNH BIỆN PHÁP BẢO MẬT EMAIL

- **Bao gồm hướng dẫn:**
- khi nào có thể chia sẻ địa chỉ email công việc của bạn
- chỉ mở tệp đính kèm email từ các địa chỉ liên hệ và doanh nghiệp đáng tin cậy
- chặn thư rác và email lừa đảo
- xác định, xóa và báo cáo các email đáng ngờ.



3. SỬ DỤNG EMAIL AN TOÀN

- **Một số quy tắc đơn giản để mở email một cách an toàn:**
- Thận trọng khi nhận được email yêu cầu cung cấp mật khẩu, thông tin đăng nhập hoặc thông tin cá nhân (đặc biệt là thông tin ngân hàng!)
- Kiểm tra xem địa chỉ email của người gửi có đáng tin cậy hay không
- Chỉ mở tệp đính kèm hoặc nhấp vào liên kết từ người gửi mà bạn biết
- Nếu không chắc chắn, hãy yêu cầu trợ giúp
- Biết rõ ai là người hỗ trợ CNTT trong trường hợp khẩn cấp
- Email không thực sự là kênh phù hợp để gửi thông tin nhạy cảm và trong trường hợp một số thông tin khác
  - ví dụ: khi xử lý Hồ sơ sinh viên – bạn bắt buộc phải sử dụng hệ thống nhắn tin bảo mật.

4. GIẢI THÍCH CÁCH XỬ LÝ DỮ LIỆU NHẠY CẢM

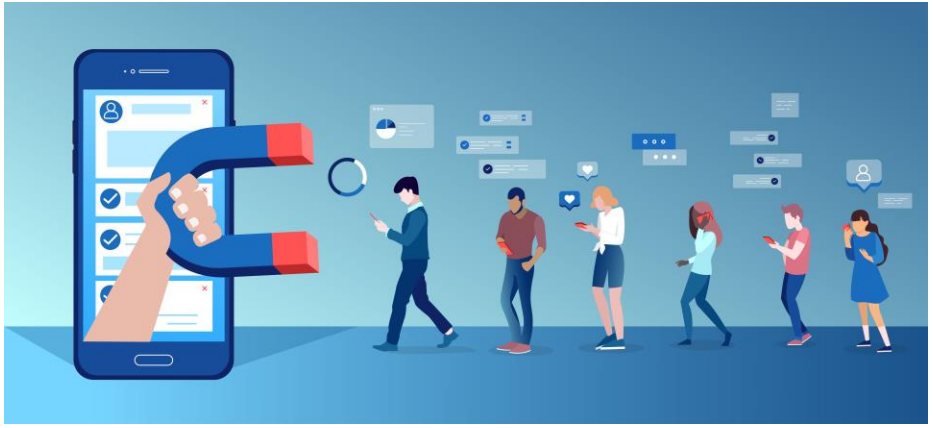
- **Liên quan đến xử lý dữ liệu nhạy cảm, cần xác định rõ:**
- khi nào nhân viên có thể chia sẻ dữ liệu nhạy cảm với người khác
- cách thức lưu trữ hồ sơ bản giấy có dữ liệu nhạy cảm, chẳng hạn như trong phòng hoặc ngăn kéo có khóa
- cách thức xác định dữ liệu nhạy cảm
- cách thức hủy dữ liệu nhạy cảm khi không còn cần thiết

5. XÁC ĐỊNH QUY TẮC VỀ SỬ DỤNG CÔNG NGHỆ

- **Các quy tắc về sử dụng công nghệ nên bao gồm:**
- địa điểm mà nhân viên có thể sử dụng thiết bị của họ, chẳng hạn như sử dụng máy tính xách tay khi không ở nơi làm việc
- cách thức cất giữ thiết bị khi không sử dụng
- cách thức báo cáo khi thiết bị làm việc bị mất trộm
- cách thức bản cập nhật hệ thống, bao gồm bản vá lỗi và bản cập nhật bộ lọc thư rác, sẽ được triển khai cho các thiết bị của nhân viên
- khi nào nên tắt máy tính và thiết bị di động nếu không sử dụng
- yêu cầu khóa màn hình khi máy tính và thiết bị không có người sử dụng
- cách thức bảo vệ dữ liệu được lưu trữ trên các thiết bị như thẻ nhớ USB
- quy định hạn chế về việc sử dụng thiết bị di động để tránh trường hợp phần mềm độc hại được cài đặt lên thiết bị
- yêu cầu quét vi-rút đối với tất cả các thiết bị di động trước khi kết nối thiết bị với hệ thống tại tổ chức của bạn

6. XÁC ĐỊNH TIÊU CHUẨN VỀ TRUY CẬP MẠNG XÃ HỘI VÀ INTERNET

- **Tiêu chuẩn về truy cập mạng xã hội và internet có thể bao gồm:**
- thông tin nào của doanh nghiệp có thể chia sẻ trên các kênh truyền thông xã hội
- nhân viên có thể truy cập vào nội dung gì bằn tài khoản email công việc của họ
- hướng dẫn về những trang web và kênh truyền thông xã hội phù hợp mà nhân viên có thể truy cập trong giờ làm việc



7. CHUẨN BỊ PHẢN HỒI SỰ CỐ

- **Nếu xảy ra sự cố an ninh mạng, bạn nên giảm thiểu tác động và phục hồi hoạt động của hệ thống càng sớm càng tốt. Bạn cần xem xét:**
- cách thức phản hồi với sự cố an ninh mạng
- hành động cần thực hiện
- vai trò và trách nhiệm của nhân viên khi phản hồi với một cuộc tấn công mạng

LẬP KẾ HOẠCH PHẢN HỒI SỰ CỐ AN NINH MẠNG

- **Chuẩn bị và ngăn ngừa**
- Giúp tổ chức và nhân viên của bạn sẵn sàng xử lý các sự cố an ninh mạng.
- Xây dựng chính sách, quy trình để giúp nhân viên hiểu rõ cách thức ngăn chặn một cuộc tấn công và xác định các sự cố tiềm ẩn.
- Xác định những tài sản quan trọng đối với tổ chức của bạn – tài sản tài chính, thông tin và công nghệ.
- Xem xét rủi ro đối với những tài sản này và các bước bạn cần thực hiện để giảm thiểu tác động của sự cố.
- Xác định rõ vai trò và trách nhiệm để mỗi người biết rõ phải báo cáo cho ai nếu xảy ra sự cố và phải làm gì tiếp theo.

LẬP KẾ HOẠCH PHẢN HỒI SỰ CỐ AN NINH MẠNG

- **Kiểm tra và phát hiện**
- **Kiểm tra và xác định các hoạt động bất thường, có thể phá hỏng thông tin và hệ thống dữ liệu tại tổ chức của bạn. Hoạt động bất thường có thể bao gồm:**
- không thể truy cập tài khoản và hệ thống mạng
- mật khẩu không hoạt động
- dữ liệu bị thiếu hoặc thay đổi
- ổ cứng hết dung lượng
- máy tính liên tục gặp sự cố
- khách hàng nhận được thư rác từ tài khoản doanh nghiệp của bạn
- bạn nhận được nhiều quảng cáo bật lên

LẬP KẾ HOẠCH PHẢN HỒI SỰ CỐ AN NINH MẠNG

- **Xác định và đánh giá**
- Tìm hiểu nguyên nhân ban đầu của sự cố và đánh giá tác động để bạn có thể nhanh chóng kiểm soát sự cố.
- Xác định tác động của sự cố đối với tổ chức của bạn.
- Xác định ảnh hưởng của sự cố đối với tổ chức và tài sản của bạn nếu không được kiểm soát ngay lập tức.

LẬP KẾ HOẠCH PHẢN HỒI SỰ CỐ AN NINH MẠNG

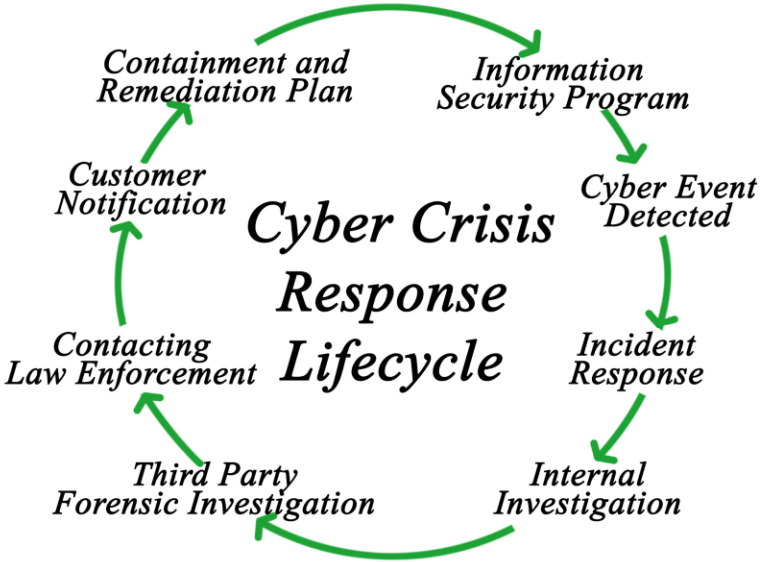
- **Phản hồi**
- Hạn chế mức độ thiệt hại của sự cố an ninh mạng bằng cách tách riêng các hệ thống bị ảnh hưởng. Nếu cần thiết, hãy ngắt kết nối mạng và tắt máy tính của bạn để ngăn ngừa mối đe dọa lây lan.
- Kiểm soát mối đe dọa.
- Phục hồi sau sự cố bằng cách sửa chữa và khôi phục hệ thống trở về mức hoạt động bình thường.

LẬP KẾ HOẠCH PHẢN HỒI SỰ CỐ AN NINH MẠNG

- **Đánh giá**
- Xác định, thực hiện những cải tiến cần thiết với hệ thống và quy trình của tổ chức.
- Đánh giá sự cố trước và sau khi phát hiện cũng như bài học kinh nghiệm.
- Cập nhật kế hoạch phản hồi sự cố an ninh mạng dựa trên bài học kinh nghiệm để có thể tăng cường năng lực phản hồi trong tổ chức.

8. CẬP NHẬT CHÍNH SÁCH THƯỜNG XUYÊN

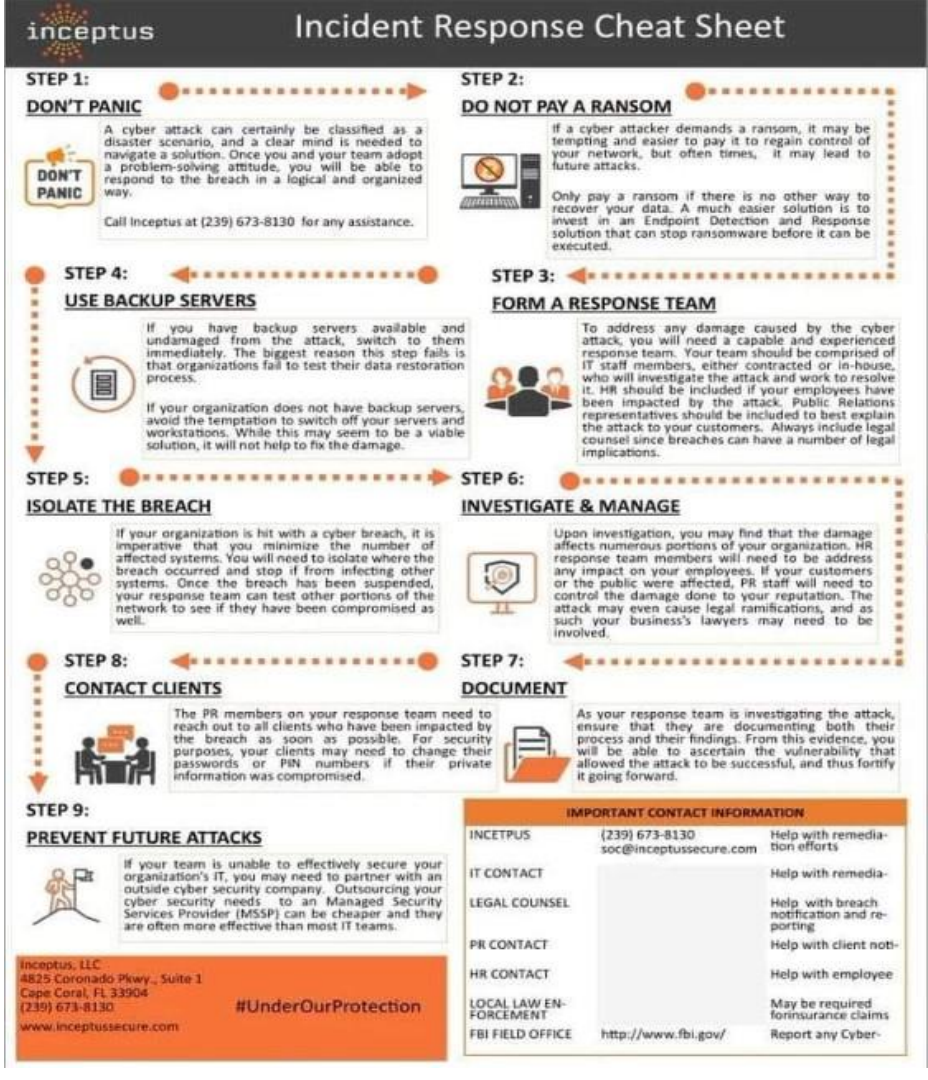
- Bạn nên xây dựng, đánh giá và cập nhật chính sách an ninh mạng một cách thường xuyên.



Australian Aid

BỘ LAO ĐỘNG - THƯƠNG BINH VÀ XÃ HỘI
TỔNG CỤC GIÁO DỤC NGHỀ NGHIỆP
DIRECTORATE OF VOCATIONAL EDUCATION AND TRAINING

- **HÃY XEM XÉT MỘT SỐ NGHIÊN CỨU ĐIỂN HÌNH TỪ:**
- Uber
- Target
- SolarWinds



AUS4SKILLS

RMIT UNIVERSITY

VẤN ĐỀ VỀ QUYỀN RIÊNG TƯ TRONG THỜI ĐẠI NGÀY NAY

- **Vấn đề về quyền riêng tư trên Internet: Theo dõi, thâm nhập và mua bán**

1. GIÁN ĐIỆP VÀ TRUY CẬP TRÁI PHÉP

- Khi bạn hoạt động trực tuyến, bạn bị một số ứng dụng theo dõi cho nhiều mục đích khác nhau.
- Ứng dụng theo dõi ghi lại lịch sử tìm kiếm và theo dõi tất cả các hoạt động trực tuyến của bạn thông qua nhiều phương tiện khác nhau. Nhờ đó, ứng dụng thu thập bức tranh rõ ràng về bạn, bao gồm sở thích của bạn, điều này vi phạm chính sách quyền riêng tư trực tuyến và khiến thông tin về bạn trở thành một tài sản chung.
- Hoạt động theo dõi này hầu như chỉ cho mục đích quảng cáo, tức giúp hiển thị quảng cáo phù hợp với sở thích và xu hướng tìm kiếm thông tin của bạn.
- Đôi khi thông tin này được tội phạm mạng sử dụng để thực hiện các hoạt động phi phép, gây rủi ro cho quá trình hoạt động trực tuyến của bạn.

2. XỬ LÝ THÔNG TIN KHÔNG ĐÚNG QUY ĐỊNH

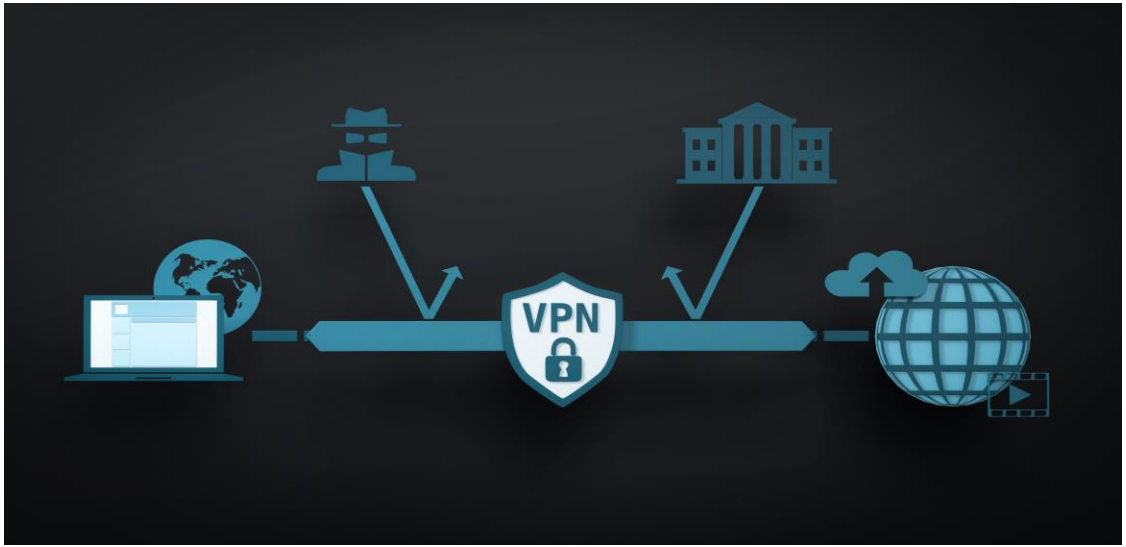
- Nhiều trang web trên internet yêu cầu bạn phải cung cấp thông tin cá nhân để sử dụng các dịch vụ của họ.
- Các trang web này thường lưu trữ cookie và thông tin cá nhân của bạn, sau đó sử dụng nó cho các mục đích khác nhau. Những tthông tin này hầu như không được mã hóa và bất kỳ ai cũng có thể truy cập được.
- Việc xử lý thông tin cá nhân không đúng quy định như vậy có thể dẫn đến nhiều hậu quả nghiêm trọng.
- Xu hướng giao dịch qua hệ thống ngân hàng điện tử và cổng thông tin của tổ chức đã làm gia tăng những rủi ro liên quan đến quyền riêng tư trực tuyến. Bằng cách chia sẻ thông tin ngân hàng và các thông tin quan trọng trên internet, bạn đang tiếp tay cho những kẻ tội phạm mạng và biến bản thân trở thành mục tiêu tấn công.

3. THEO DÕI VỊ TRÍ

- Trong các bài đăng lên mạng xã hội, hầu hết người dùng internet thường gắn vị trí hiện tại của họ cũng như gắn thẻ bạn bè và thành viên gia đình.
- Chúng ta đều mong muốn được chia sẻ những sự kiện trong cuộc sống với bạn bè và gia đình, nhưng việc truy cập dữ liệu này không chỉ giới hạn đối với đối tượng mục tiêu của bạn.
- Dữ liệu này cũng được lưu trữ mãi mãi trên trang mạng xã hội mà bạn đang sử dụng mà bạn thường không biết (mặc dù bạn có thể đã đồng ý với điều khoản và yêu cầu sử dụng dịch vụ).
- Cùng với ứng dụng mạng xã hội, Google Maps và các ứng dụng khác cũng yêu cầu bạn xác định vị trí và bằng cách bật vị trí của mình, bạn đang cung cấp thông tin trực tiếp cho cả thế giới về vị trí chính xác của bạn và địa điểm di chuyển tiếp theo, và đây có thể là rủi ro với an toàn của bạn.

4. GIẢI PHÁP BẢO VỆ TRƯỚC CÁC MỐI ĐE DỌA VỀ QUYỀN RIÊNG TƯ TRỰC TUYẾN

- Sử dụng VPN
- Tiến hành duyệt web an toàn
- Luôn cập nhật hệ thống của bạn
- Sử dụng phần mềm chống virus
- Điều chỉnh cài đặt của bạn trên trang mạng xã hội cá nhân
- Hạn chế đăng bài trên các trang mạng xã hội ở mức tối thiểu
- Sử dụng dịch vụ đám mây cho công việc hàng ngày



BẢO MẬT ĐÁM MÂY VÀ PHẦN MỀM ĐỘC HẠI

- Tổng quan về bảo mật đám mây

VAI TRÒ CỦA BẢO MẬT ĐÁM MÂY?

- Khi càng nhiều doanh nghiệp chuyển sang dịch vụ đám mây, kiến thức về yêu cầu bảo mật để bảo vệ dữ liệu an toàn có vai trò rất quan trọng.
- Mặc dù các nhà cung cấp điện toán đám mây bên thứ ba có thể đảm nhận vai trò quản lý hạ tầng đám mây, họ không nhất thiết phải có trách nhiệm bảo mật tài sản dữ liệu và trách nhiệm giải trình.

MỘT SỐ THÁCH THỨC BẢO MẬT CỦA ĐIỆN TOÁN ĐÁM MÂY?

- **Thiếu khả năng hiển thị**
  Thường không thể theo dõi mục đích và đối tượng dữ liệu của bạn, vì nhiều dịch vụ đám mây được truy cập bên ngoài mạng công ty và thông qua bên thứ ba.

- **Đa mạng**
  Môi trường đám mây công cộng bao gồm nhiều cơ sở hạ tầng máy khách trên một máy chủ, vì vậy các dịch vụ lưu trữ của bạn có thể bị tấn công, gây ra những thiệt hại ngoài dự kiến khi hướng tới mục tiêu tấn công vào các doanh nghiệp khác.

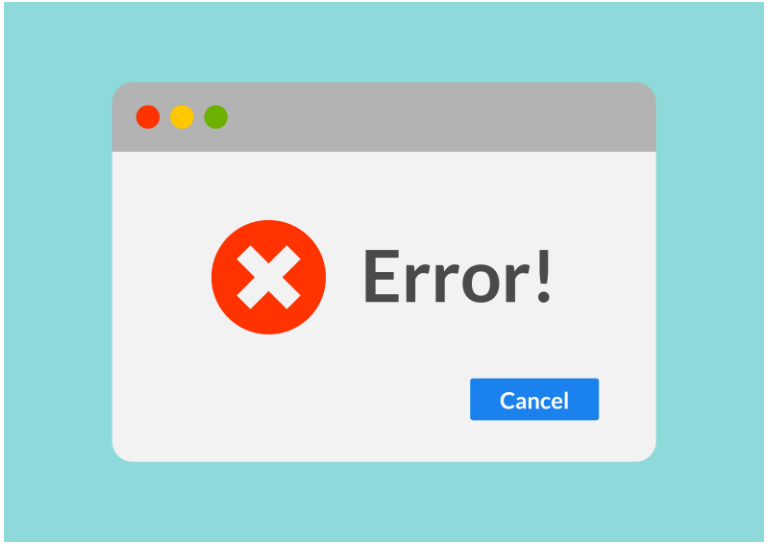
- **Quản lý truy cập và công cụ, phần mềm không được quy định (shadow IT)**
  Dù có thể quản lý và hạn chế các điểm truy cập trên hệ thống của mình, doanh nghiệp có thể gặp nhiều khó khăn khi quản lý truy cập trong môi trường đám mây. Đây có thể rủi ro với các tổ chức không triển khai chính sách với thiết bị cá nhân và cho phép đối tượng truy cập, dù chưa sàng lọc kỹ càng, tiếp cận các dịch vụ đám mây từ bất kỳ thiết bị hoặc vị trí địa lý nào.

- **Tuân thủ**
  Doanh nghiệp đôi khi gặp khó khăn khi quản lý tuân thủ pháp luật trên các nền tảng đám mây công cộng hoặc đám mây kết hợp. Doanh nghiệp vẫn có trách nhiệm đảm bảo quyền riêng tư và bảo mật dữ liệu; do đó, việc phụ thuộc quá nhiều vào các giải pháp của bên thứ ba để quản lý tuân thủ có thể khiến chi phí tuân thủ khá lớn.

MỘT SỐ THÁCH THỨC BẢO MẬT CỦA ĐIỆN TOÁN ĐÁM MÂY?

- **Lỗi cấu hình sai**

  Lỗi cấu hình sai chiếm 86% trường hợp rò rỉ dữ liệu vào năm 2019, khiến mối đe dạo nội bộ vô tình trở thành vấn đề chính khi hoạt động trong môi trường điện toán đám mây. Lỗi cấu hình sai có thể bao gồm để nguyên mật khẩu quản trị mặc định hoặc không thực hiện cài đặt quyền riêng tư phù hợp.

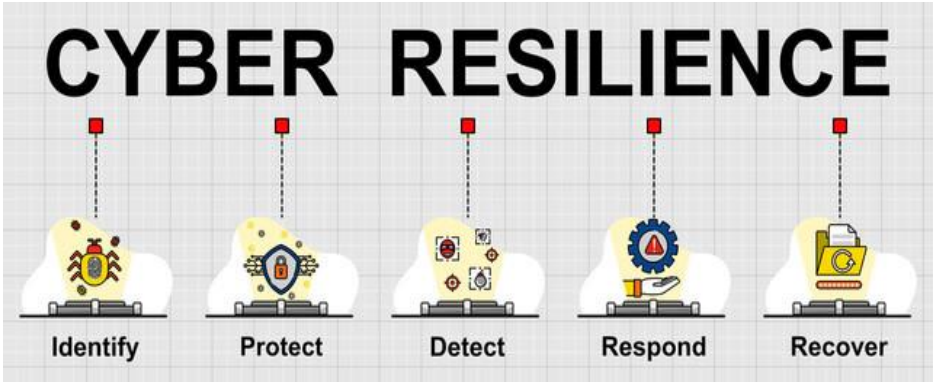


CÁC NHÓM GIẢI PHÁP BẢO MẬT ĐÁM MÂY?

- Quản lý danh tính và quyền truy cập (IAM)
- Chống thất thoát dữ liệu (DLP)
- Quản lý sự kiện và thông tin bảo mật (SIEM)
- Tính liên tục trong kinh doanh và khôi phục dữ liệu sau thả
- Hạ tầng khóa công khai (PKI):
- Triển khai xác thực hai yếu tố

BẠN NÊN TIẾP CẬN TRIỂN KHAI BẢO MẬT ĐÁM MÂY NHƯ THẾ NÀO?

- NIST đã xây dựng các bước cần thiết để mọi tổ chức có thể tự đánh giá mức độ bảo mật và áp dụng các biện pháp bảo mật phòng ngừa và khôi phục thích hợp cho hệ thống của họ.
- Những nguyên tắc này được xây dựng dựa trên năm trụ cột của NIST cho khung an ninh mạng: **Xác định, Bảo vệ, Phát hiện, Phản hồi và Khôi phục**



PHẦN MỀM ĐỘC HẠI CÓ THỂ XÂM NHẬP VÀO NỀN TẢNG ĐÁM MÂY NHƯ THẾ NÀO?

- Nền tảng đám mây an toàn hơn máy chủ tại chỗ vì nhiều lý do khác nhau, từ độ bền dữ liệu cao hơn đến quản lý bản vá nhất quán hơn — nhưng dù là như vậy, doanh nghiệp vẫn gặp nhiều mối đe dọa với bảo mật đám mây. Phần mềm độc hại dựa trên nền tảng đám mây là một trong số đó.
- Phần mềm độc hại, được phát tán thông qua các ứng dụng lưu trữ đám mây như Microsoft OneDrive, Google Drive và Box, chiếm 69% lượt tải xuống phần mềm độc hại trên nền tảng đám mây

BỐN PHƯƠNG PHÁP TỐT NHẤT ĐỂ NGĂN CHẶN PHẦN MỀM ĐỘC HẠI DỰA TRÊN NỀN TẢNG ĐÁM MÂY

- **1. Khắc phục lỗ hổng trong bảo mật đám mây**

- Khắc phục lỗ hổng trong bảo mật đám mây được coi là một trong những lớp phòng vệ đầu tiên chống lại phần mềm độc hại dựa trên nền tảng đám mây. Ba giải pháp hiệu quả nhất bao gồm:

- Triển khai chính sách hiệu quả về quản lý danh tính và quyền truy cập (IAM):
- Cấu hình phù hợp các API công khai:
- Thiết lập đúng hệ thống lưu trữ đám mây:

BỐN PHƯƠNG PHÁP TỐT NHẤT ĐỂ NGĂN CHẶN PHẦN MỀM ĐỘC HẠI DỰA TRÊN NỀN TẢNG ĐÁM MÂY

- **2. Bảo vệ điểm cuối để phát hiện và kiểm soát phần mềm độc hại trước khi phần mềm này xâm nhập vào nền tảng đám mây**
- Một trong số hàng trăm điểm cuối đều có thể bị nhiễm phần mềm độc hại vào bất kỳ thời điểm nào. Và nếu bạn không thể phát hiện và kiểm soát phần mềm độc hại ngay khi điểm cuối bị lây nhiễm, phần mềm này có thể đồng bộ hóa với OneDrive — và khi đó có thể lây nhiễm sang nhiều tệp hơn.
- Ba tính năng phát hiện và phản hồi mối nguy hại tại điểm cuối có thể giúp t
  loại bỏ phần mềm độc hại:
- Giám sát hoạt động đáng ngờ:
- Cô lập tấn công
- Phản hồi sự cố

BỐN PHƯƠNG PHÁP TỐT NHẤT ĐỂ NGĂN CHẶN PHẦN MỀM ĐỘC HẠI DỰA TRÊN NỀN TẢNG ĐÁM MÂY

- **3. Sử dụng trình quét lưu trữ đám mây ở lớp thứ 2 để phát hiện phần mềm độc hại dựa trên nền tảng đám mây**
- Ngay cả khi bạn đã khắc phục tất cả các lỗ hổng trong bảo mật đám mây của mình và sử dụng một sản phẩm EDR hàng đầu, phần mềm độc hại vẫn có thể xâm nhập vào nền tảng đám mây — và đó là lý do cần thực hiện quét lưu trữ đám mây thường xuyên.

BỐN PHƯƠNG PHÁP TỐT NHẤT ĐỂ NGĂN CHẶN PHẦN MỀM ĐỘC HẠI DỰA TRÊN NỀN TẢNG ĐÁM MÂY

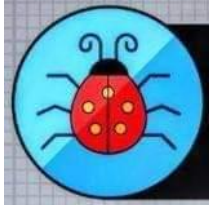
- **4. Có chiến lược sao lưu dữ liệu**

- Trường hợp xấu nhất: Bạn đã định cấu hình đám mây của mình đúng cách, bảo mật tất cả điểm cuối và thường xuyên quét hệ thống đám mây — nhưng phần mềm độc hại dựa trên nền tảng đám mây vẫn tìm cách vượt qua hệ thống bảo vệ và mã hóa tất cả các tệp của bạn.
- Bạn nên có một chiến lược sao lưu dữ liệu cho đúng kịch bản bị tấn công mã độc như vậy.
- Khi nói đến các cuộc tấn công mã độc trên đám mây — khiến doanh nghiệp mất dữ liệu quan trọng hoặc nhạy cảm — chiến lược sao lưu dữ liệu là giải pháp tốt nhất để khôi phục các tệp bị mất.

Australian Aid

BỘ LAO ĐỘNG - THƯƠNG BINH VÀ XÃ HỘI
TỔNG CỤC GIÁO DỤC NGHỀ NGHIỆP
DIRECTORATE OF VOCATIONAL EDUCATION AND TRAINING

Types of Malware

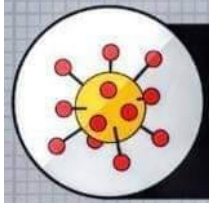


BUGS

A type of error, flaw or failure that produces an undesirable or unexpected result. Bugs typically exist in a website's source code and can cause a wide range of damage.

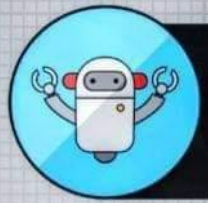
WORMS

A worm relies on security failures to replicate and spread itself to other computers. They are often hidden in attachments and will consume bandwidth and overload a web server.



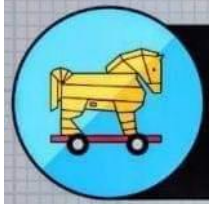
VIRUS

A piece of code that is loaded onto your website or computer without your knowledge. It can easily multiply and be transmitted as an attachment or file.



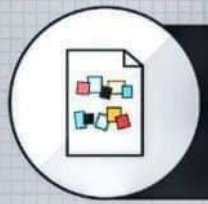
BOTS

A software program created to perform specific tasks. Bots can send spam or be used in a DDoS attack to bring down an entire website.



TROJAN HORSES

Much like the myth, a Trojan disguises itself as a normal file and tricks users into downloading it, consequently installing malware.



RANSOMWARE

Ransomware denies access to your files and demands payment through Bitcoin in order for access to be granted again.

ADWARE

A type of malware that automatically displays unwanted advertisements. Clicking on one of these ads could redirect you to a malicious site.

SPYWARE

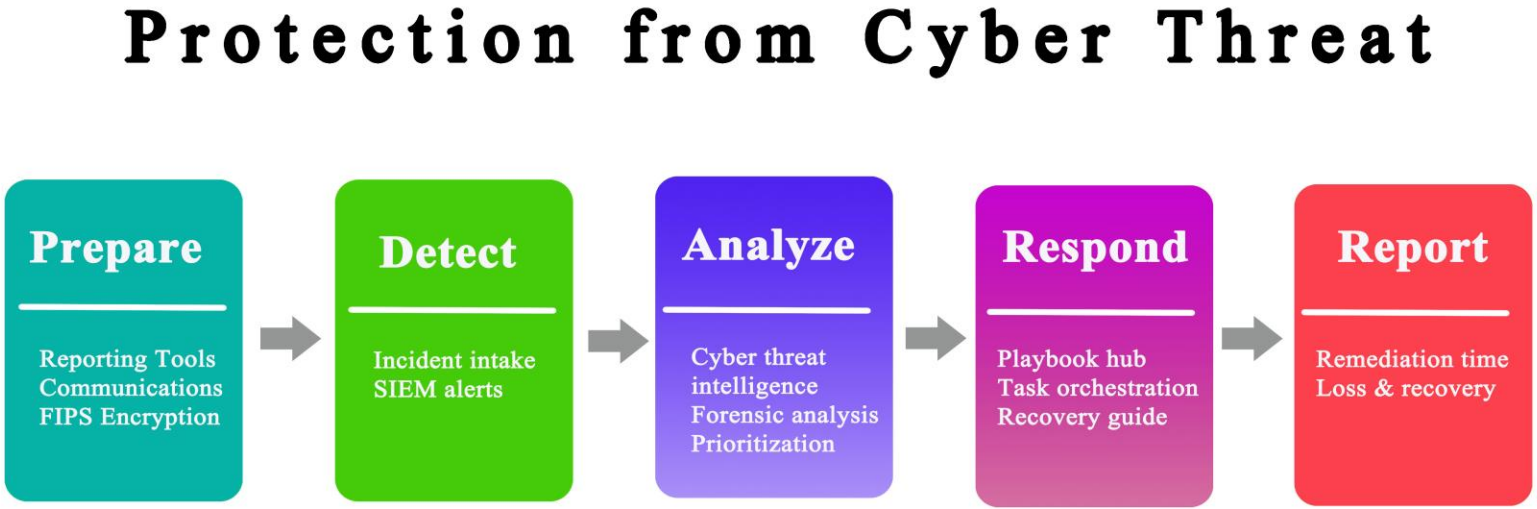
A type of malware that functions by spying on a user's activity. This type of spying includes monitoring a user's activity, keystrokes and more.

AUS4SKILLS

RMIT UNIVERSITY

THÔNG TIN MỐI ĐE DỌA AN NINH MẠNG

- Thông tin mối đe dọa an ninh mạng là dữ liệu được thu thập, xử lý và phân tích để hiểu động cơ, mục tiêu và hành vi tấn công của tác nhân đe dọa



THÔNG TIN MỐI ĐE DỌA AN NINH MẠNG

- Để bảo vệ hiệu quả khỏi các cuộc tấn công mạng, trước tiên phải hiểu rõ kỹ thuật và phương thức tấn công. Thông tin mối đe dọa an ninh mạng phục vụ cho mục tiêu quan trọng này: đảm bảo tính phù hợp của các lớp phòng vệ. Tội phạm mạng nhắm vào các hoạt động kinh doanh và hệ thống CNTT, do đó, cần hiểu rõ các mối đe dọa đó để thực hiện giải pháp phù hợp cho từng khách hàng.
- Thông tin mối đe dọa an ninh mạng giúp thu thập, phân tích và sau đó sắp xếp tất cả dữ liệu liên quan đến một cuộc tấn công mạng, kẻ tấn công và các quy trình được sử dụng. Thông tin mối đe dọa an ninh mạng đòi hỏi nỗ lực của nhiều bên liên quan vì nó cho phép mỗi bên mở rộng kiến thức về các cuộc tấn công và tự bảo vệ bản thân họ hiệu quả hơn.

QUẢN LÝ SỰ KIỆN VÀ THÔNG TIN BẢO MẬT

- **SIEM hoạt động như thế nào?**
- SIEM thu thập thông tin từ nhật ký và dữ liệu sự kiện do một tổ chức tạo ra trên các ứng dụng, hệ thống bảo mật và phần cứng của tổ chức đó. Bằng cách kết hợp sự kiện với các quy tắc và công cụ phân tích, hệ thống SIEM có thể phát hiện và phân tích các mối đe dọa bảo mật theo thời gian thực. Tất cả thông tin đều được lập chỉ mục để hỗ trợ các nhóm bảo mật tìm kiếm, phân tích, quản lý nhật ký và báo cáo.

VÍ DỤ VỀ CÁC MỐI ĐE DỌA MÀ GIẢI PHÁP SIEM CÓ THỂ PHÁT HIỆN

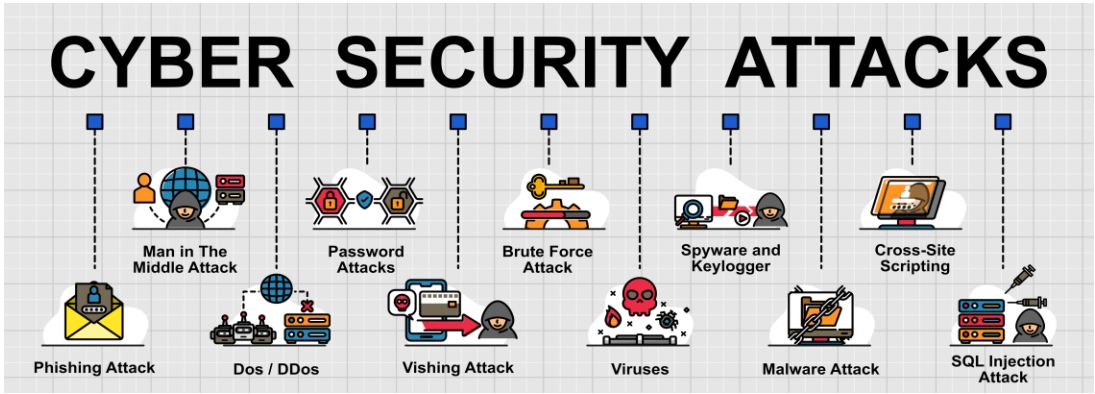
- **Truy cập trái phép**
- Người dùng có thể đăng nhập hệ thống không thành công một vài lần. Nếu số lần đăng nhập không thành công lên đến 100 lần, ai đó có thể đang thực hiện tấn công theo phương thức thử sai. Phần mềm SIEM có thể theo dõi hành vi của người dùng và xác định các hành vi truy cập bất thường.
- **Mối đe dọa nội bộ**
- Bằng cách liên tục theo dõi hành vi của nhân viên, hệ thống SIEM có thể phát hiện các mối đe dọa nội bộ, cả vô tình và độc hại. Từ nhân viên cũ chưa bị thu hồi quyền truy cập, cho đến những kẻ nội gián đang cố gắng đánh cắp hoặc rò rỉ thông tin nhạy cảm, hay những thay đổi vô tình về bảo mật, phần mềm SIEM có thể phát hiện và báo cáo hành vi bất thường cho chuyên gia phân tích bảo mật để thực hiện phân tích.

VÍ DỤ VỀ CÁC MỐI ĐE DỌA MÀ GIẢI PHÁP SIEM CÓ THỂ PHÁT HIỆN

- **Lừa đảo**
- Các cuộc tấn công lừa đảo được thực hiện bằn cách mạo danh một tổ chức uy tín, với mục đích để nạn nhân tự nguyện tiết lộ thông tin cá nhân hoặc thông tin nhạy cảm.
- **Tấn công DoS và DDoS**
- Tấn công từ chối dịch vụ (DoS) làm gián đoạn các dịch vụ bằng cách gây nghẽn mạng để không thể truy cập tài nguyên hệ thống và gây ra sự cố.
- **Chèn mã độc**
- Chèn mã độc là hành vi đưa mã độc vào các trang thông tin đầu vào phía máy khách, chẳng hạn như biểu mẫu trực tuyến, để có quyền truy cập vào cơ sở dữ liệu hoặc hệ thống của ứng dụng.

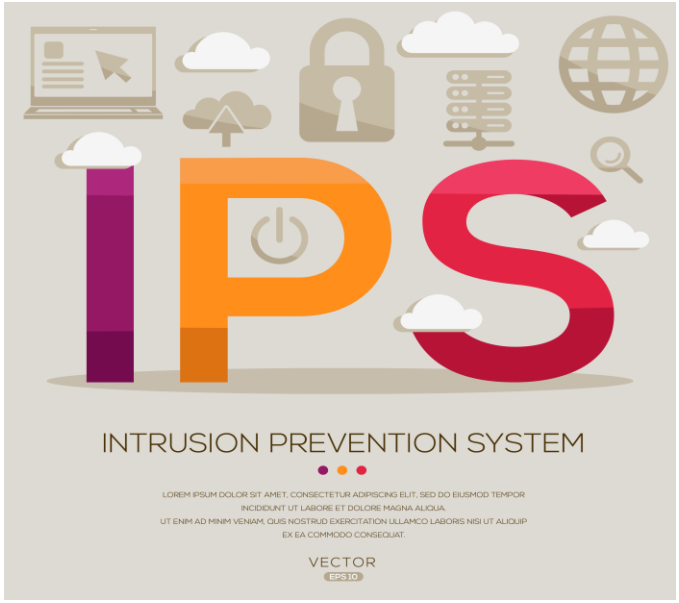
VÍ DỤ VỀ CÁC MỐI ĐE DỌA MÀ GIẢI PHÁP SIEM CÓ THỂ PHÁT HIỆN

- **Mã độc và phần mềm độc hại khác**
- Mã độc, vi rút, sâu máy tính, trojan và các phần mềm độc hại khác là phần mềm được thiết kế để xâm nhập vào hệ thống máy tính và thực thi các chương trình độc hại.
- **Tấn công MITM**
- Tấn công xen giữa (MITM) xảy ra khi một bên thứ ba nghe trộm thông tin liên lạc giữa hai máy chủ để đánh cắp hoặc thao túng thông tin.



CÁC NHÀ CUNG CẤP GIẢI PHÁP AN NINH MẠNG SIEM PHỔ BIẾN

- **Một số công cụ SIEM phổ biến trên thị trường bao gồm:**
- Elastic SIEM
- SolarWinds SIEM
- Datadog
- Splunk Enterprise SIEM
- McAfee ESM
- Micro Focus ArcSight
- LogRhythm
- Giải pháp an ninh mạng SIEM của AT&T (Trước đây là AlienVault USM)
- RSA NetWitness
- Netsurion EventTracker

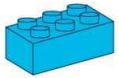
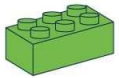
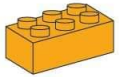
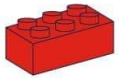
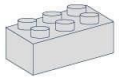


Australian Aid

BỘ LAO ĐỘNG - THƯƠNG BINH VÀ XÃ HỘI
TỔNG CỤC GIÁO DỤC NGHỀ NGHIỆP
DIRECTORATE OF VOCATIONAL EDUCATION AND TRAINING

TƯỜNG LỬA

Save this post to remember the types of firewall

 Proxy firewall	An early type of device, serves as the gateway from one network to another for a specific application
 Stateful inspection firewall	Now thought of as a “traditional”, allows or blocks traffic based on state, port, and protocol
 Unified threat management (UTM) firewall	Typically combines the functions of a stateful inspection firewall with intrusion prevention and antivirus
 Next-generation firewall (NGFW)	The evolution beyond simple packet filtering and stateful inspection. This blocks advanced malware and application-layer attacks
 Threat-focused NGFW	Includes all the capabilities of a traditional NGFW and also provides advanced threat detection and remediation
 Virtual firewall	Is typically deployed as a virtual appliance in a private or public cloud to monitor and secure traffic across physical and virtual networks
 Cloud Native Firewall	With automated scaling features, enables networking operations and security operations teams to run at agile speeds

AUS4SKILLS

RMIT UNIVERSITY

Networking Academy

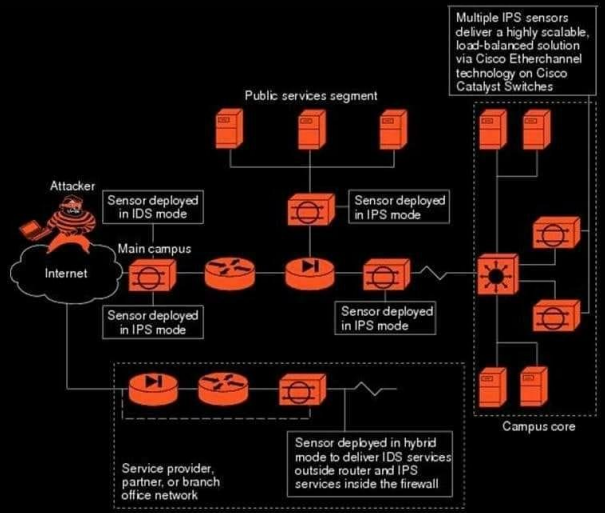
Australian Aid

BỘ LAO ĐỘNG - THƯƠNG BINH VÀ XÃ HỘI
TỔNG CỤC GIÁO DỤC NGHỀ NGHIỆP
DIRECTORATE OF VOCATIONAL EDUCATION AND TRAINING

IDS Vs IPS

Most organizations have either an IDS or an IPS, and many have both as part of their security information and event management framework.

	IDS	IPS
NAME	Intrusion detection system	Intrusion prevention system
DESCRIPTION	A system that monitors network traffic for suspicious activity and alerts users when such activity is discovered.	A system that monitors network traffic and alerts for suspicious activity, like an IDS, but also takes preventative action against suspicious activity.
LOCATION	A host-based intrusion detection system is installed on the client computer. A network-based intrusion detection system resides on the network.	Located between a company's firewall and the rest of its network.
USE	Warns of suspicious activity taking place, but it doesn't prevent it.	Warns of suspicious activity taking place and prevents it.
FALSE POSITIVE	IDS false positives are usually just a minor inconvenience. Although the IDS incorrectly labels legitimate traffic as malicious, it does not prevent the traffic from entering the network.	IPS false positives can be more serious. When an IPS mistakes legitimate traffic for a threat, it stops the legitimate traffic from entering the network, which could impact any part of the organization, not just the IT team.



How to place Sensors correctly for IPS

AUS4SKILLS

RMIT UNIVERSITY

Australian Aid

BỘ LAO ĐỘNG - THƯƠNG BINH VÀ XÃ HỘI
TỔNG CỤC GIÁO DỤC NGHỀ NGHIỆP
DIRECTORATE OF VOCATIONAL EDUCATION AND TRAINING

Top 5 Password Attack Types

Cyber Writes

Brute Force Attack

A brute force attack is a type of password crack that uses a computer program to generate and try every possible combination of characters until it finds the correct password. This attack is very time-consuming and often requires large amounts of computing power, but it can be successful if the attacker has enough time and resources.

Dictionary Attack

A dictionary attack is a type of password crack that uses a list of words (usually taken from a dictionary) to generate and try possible password combinations. This attack can be successful if the password is a common word or phrase, but it is much less likely to succeed if the password is a random string of characters.

Rainbow Table Attack

A rainbow table attack is a type of password crack that uses a pre-computed table of all possible hashes of all possible passwords (or a subset thereof). This attack can be very effective if the attacker has a copy of the rainbow table, but it is much less likely to succeed if the password is a random string of characters.

Social Engineering Attack

A social engineering attack is a type of password crack that relies on tricking the user into revealing their password. This attack can be successful if the attacker is skilled at deception, but it is muuch less likely to succeed if the user is aware of the risks.

credential stuffing Attack

A credential stuffing attack is a type of password crack that uses a list of stolen usernames and passwords (usually obtained from an external data breach) to try and gain access to other accounts. This attack can be successful if the user re-uses passwords across multiple accounts, but it is much less likely to succeed if the user has a unique password for each account.

AUS4SKILLS

RMIT UNIVERSITY

Australian Aid

BỘ LAO ĐỘNG - THƯƠNG BINH VÀ XÃ HỘI
TỔNG CỤC GIÁO DỤC NGHỀ NGHIỆP
DIRECTORATE OF VOCATIONAL EDUCATION AND TRAINING

20 Ways to Block Mobile Attacks

Don't let your guard down just because you're on a mobile device. Be just as careful as you would on a desktop!

WiFi

- Don't allow your device to auto-join unfamiliar networks.
- Always turn off WiFi when you aren't using it or don't need it.
- Never send sensitive information over WiFi unless you're absolutely sure it's a secure network.

Apps

- Only use apps available in your device's official store - NEVER download from a browser.
- Be wary of apps from unknown developers or those with limited/bad reviews.
- Keep them updated to ensure they have the latest security.
- If they're no longer supported by your store, just delete!
- Don't grant administrator, or excessive privileges to apps unless you truly trust them.

Browser

- Watch out for ads, giveaways and contests that seem too good to be true. Often these lead to phishing sites that appear to be legit.
- Pay close attention to URLs. These are harder to verify on mobile screens but it's worth the effort.
- Never save your login information when you're using a web browser.

Bluetooth

- Disable automatic Bluetooth pairing.
- Always turn it off when you don't need it.

Smishing (phishing via SMS)

- Don't trust messages that attempt to get you to reveal any personal information
- Beware of similar tactics in platforms like What's App, Facebook Messenger Instagram, etc.
- Treat messages the same way you would treat email, always think before you click!

Vishing (voice phishing)

- Do not respond to telephone or email requests for personal financial information. If you are concerned, call the financial institution directly, using the phone number that appears on the back of your credit card or on your monthly statement.
- Never click on a link in an unsolicited commercial email.
- Speak only with live people when providing account information, and **only** when you initiate the call.
- Install software that can tell you whether you are on a secure or fake website.

AUS4SKILLS

RMIT UNIVERSITY

KnowBe4
Human error. Conquered.

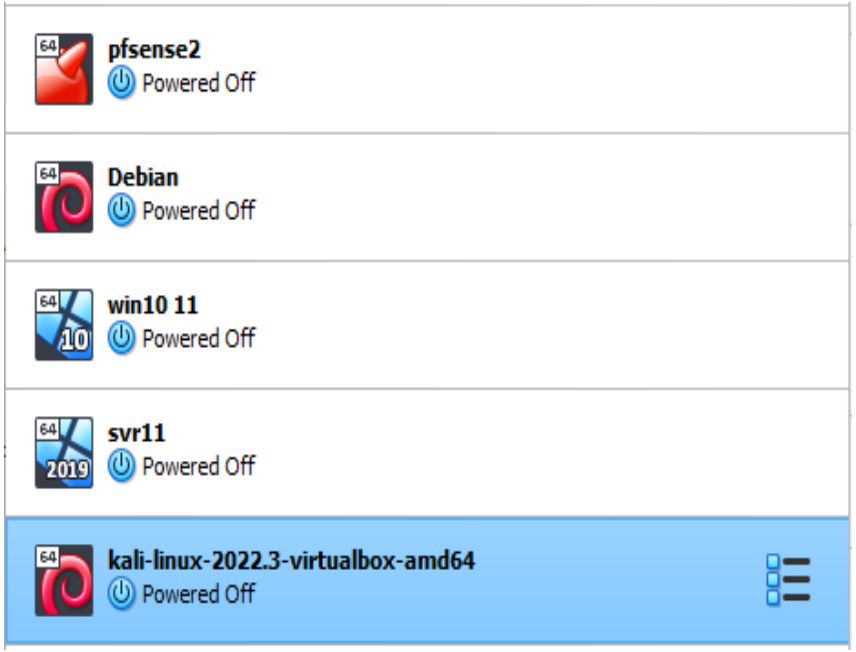
THIẾT KẾ PHÒNG THÍ NGHIỆM THỰC TẾ

- **Slide sau đây trình bày thiết kế phòng thí nghiệm cuối cùng cho dự án Phát triển an ninh mạng của RMIT:**
- Thiết kế này bao gồm thiết lập Tường lửa (pfsense)
- Công cụ SIEM ELK trên Debian 12
- Một bộ điều khiển miền với một máy khách đã tham gia vào miền.
- Một máy chủ proxy được cài đặt trong môi trường (cc proxy)
- Và một máy tính tấn công để thực hiện một vài cuộc tấn công đơn giản.
- Mục đích của thiết kế này là để sinh viên hiểu cách thiết lập một môi trường kèm các công cụ phù hợp.

THIẾT KẾ PHÒNG THÍ NGHIỆM THỰC TẾ

- Sinh viên xây dựng phòng thí nghiệm trong suốt khóa học, sau đó xây dựng lại phòng thí nghiệm trong 5 tuần và giải thích quá trình thực hiện.
- Đối với nhóm chuyên gia an ninh mạng và hệ thống bảo mật
- Sinh viên sẽ thiết lập tường lửa với IPS (SNORT) và đánh giá mức độ hoạt động.
- Sau đó, sinh viên nâng cấp máy chủ Windows thành bộ điều khiển miền và kết nối máy tính với miền, sau đó cài đặt máy chủ proxy (cc proxy) vào miền.
- Sau đó, sinh viên thiết lập công cụ SIEM trong Debian và gửi tệp nhật ký từ máy chủ đến ELK stack bằng công cụ có tên winlogbeat.
- Sau khi hoàn thành xong, tiến hành một số cuộc tấn công để đánh giá vị trí lỗ hổng trong hệ thống mạng.
- Sau đó tiến hành thảo luận trong nhóm.

THIẾT KẾ PHÒNG THÍ NGHIỆM THỰC TẾ



- Tường lửa
- ELK stack trên máy tính
- Linux đã cài đặt SIEM
- Máy khách Windows
- Máy chủ (bộ điều khiển miền)
- Máy tính tấn công

Australian Aid

BỘ LAO ĐỘNG - THƯƠNG BINH VÀ XÃ HỘI
TỔNG CỤC GIÁO DỤC NGHỀ NGHIỆP
DIRECTORATE OF VOCATIONAL EDUCATION AND TRAINING

XIN CẢM ƠN!
HỎI & ĐÁP

Các câu hỏi xin gửi về michael.barton2@rmit.edu.au

Thứ Bảy, 26/8/2023