WHEN TRUST MATTERS

Các yêu cầu quy định về an ninh mạng – Phần 1

Quản lý an ninh mạng trong ngành điện

DNV Singapore

07 August 2025



Nội dung

1. Yêu cầu về Kiểm toán và Quản trị
2. Yêu cầu về Nhận diện và Bảo vệ

1. Yêu cầu về Kiểm toán và Quản trị

DNV ©

Yêu cầu về kiểm toán

- *Những phát hiện từ hoạt động kiểm toán cần được ưu tiên và khắc phục kịp thời*
- *Đơn vị vận hành hạ tầng thông tin trọng yếu (CIIO) phải có kế hoạch khắc phục trong vòng 30 ngày làm việc*



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Yêu cầu về quản trị – Lãnh đạo và giám sát

- *Vai trò và trách nhiệm của an ninh mạng hạ tầng thông tin trọng yếu (CII) được quy định bằng văn bản VÀ được phân công rõ ràng.*
- *Ít nhất một thành viên có kiến thức và nhận thức về các vấn đề an ninh mạng*
  - *Hội đồng quản trị*
  - *Ban quản lý cấp cao*



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Yêu cầu về quản trị – Đánh giá rủi ro

- *CIIO phải thiết lập và triển khai khung quản lý rủi ro an ninh mạng*
- *Phương pháp đánh giá rủi ro an ninh mạng*
- *Bao gồm các phương thức kiểm soát kỹ thuật phi kỹ thuật số như các biện pháp kiểm soát giảm thiểu*
- *Duy trì và cập nhật sổ đăng ký rủi ro cho mỗi CII*
- *Sổ đăng ký rủi ro được rà soát và theo dõi thường xuyên*



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Khung quản lý rủi ro an ninh mạng

- *Thúc đẩy văn hóa quản lý rủi ro*
- *Vai trò và trách nhiệm của nhân sự*
- *Quy trình giám sát, truyền thông và báo cáo rủi ro an ninh mạng*
- *mức độ chấp nhận rủi ro an ninh mạng và ngưỡng hoặc giới hạn đối với rủi ro còn lại*
- *Phương pháp phân tích nguy cơ của quy trình (PHA) cho hệ thống OT*

Phương pháp đánh giá rủi ro an ninh mạng

- *Nhận diện rủi ro*
  - *Nhận diện tài sản*
  - *Nhận diện mối đe dọa*
    - *Mô hình hóa mối đe dọa*
    - *Săn tìm mối đe dọa*
    - *Đánh giá sau sự cố*
    - *Xây dựng kịch bản rủi ro*
- *Phân tích rủi ro*
  - *Khả năng xảy ra*
  - *Tác động tiềm ẩn*
- *Đánh giá rủi ro*
  - *Lập ưu tiên*
- *Ứng phó với rủi ro*
  - *Xử lý và theo dõi*
  - *Duy trì trong mức rủi ro có thể chấp nhận*

DNV ©

Tổng quan về quản lý rủi ro

DNV ©

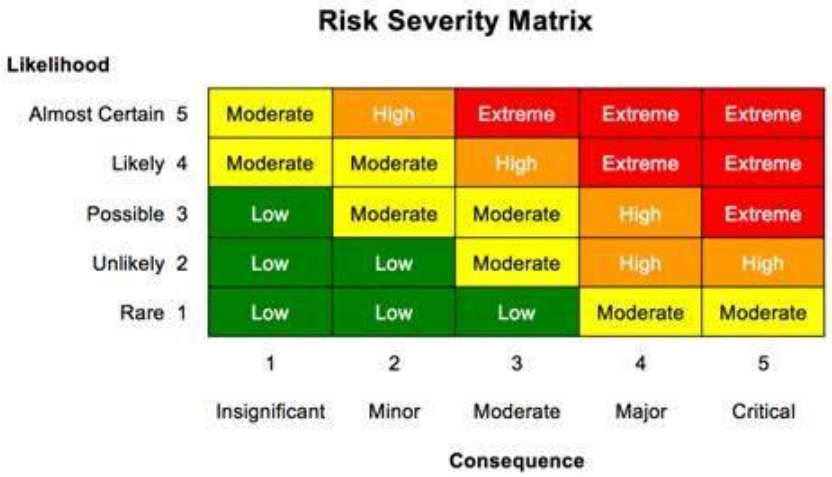
Quản lý rủi ro

Quản lý rủi ro là trọng tâm của một hệ thống an ninh mạng mạnh mẽ.

Các phương pháp phổ biến bao gồm:

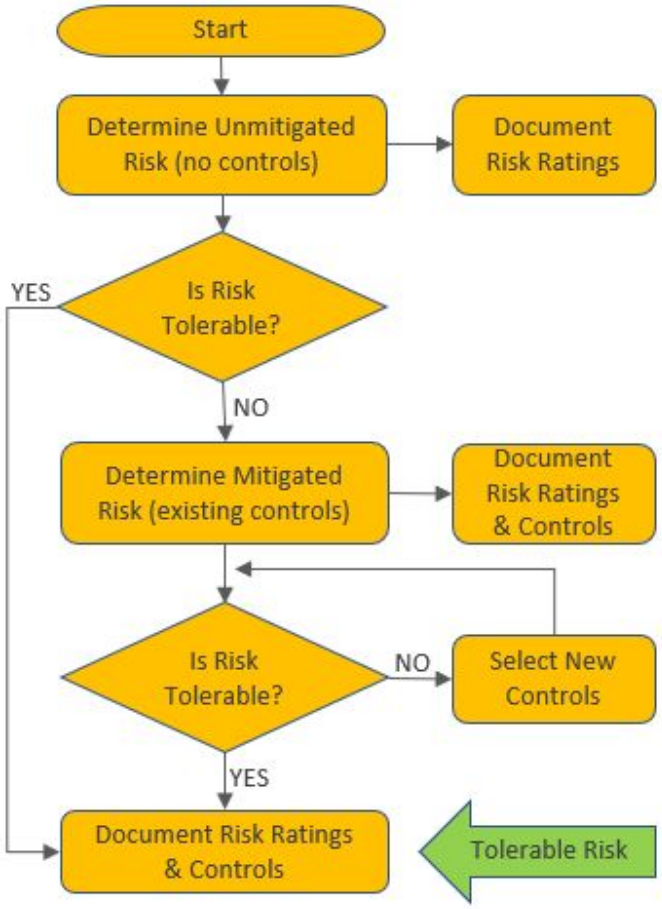
1. Cách tiếp cận dựa trên sự tuân thủ
2. Cách tiếp cận dựa trên mối nguy
3. Cách tiếp cận dựa trên rủi ro







Quy trình quản lý rủi ro chung



- Xác định và ưu tiên các tài sản/hệ thống
- Xác định các kịch bản rủi ro
  - Lập mô hình mối nguy và phân tích lỗ hổng
  - Sử dụng các rủi ro cấp độ cao đã được xác định từ những đánh giá rủi ro doanh nghiệp
- Xác định hậu quả không thể khắc phục của kịch bản rủi ro
- Xác định điểm rủi ro và thiết lập ưu tiên rủi ro
- Xác định và áp dụng các biện pháp kiểm soát an ninh để giảm rủi ro xuống mức phù hợp

Bản đồ nhiệt

- Các bên cần thống nhất về ma trận rủi ro và mức độ chấp nhận

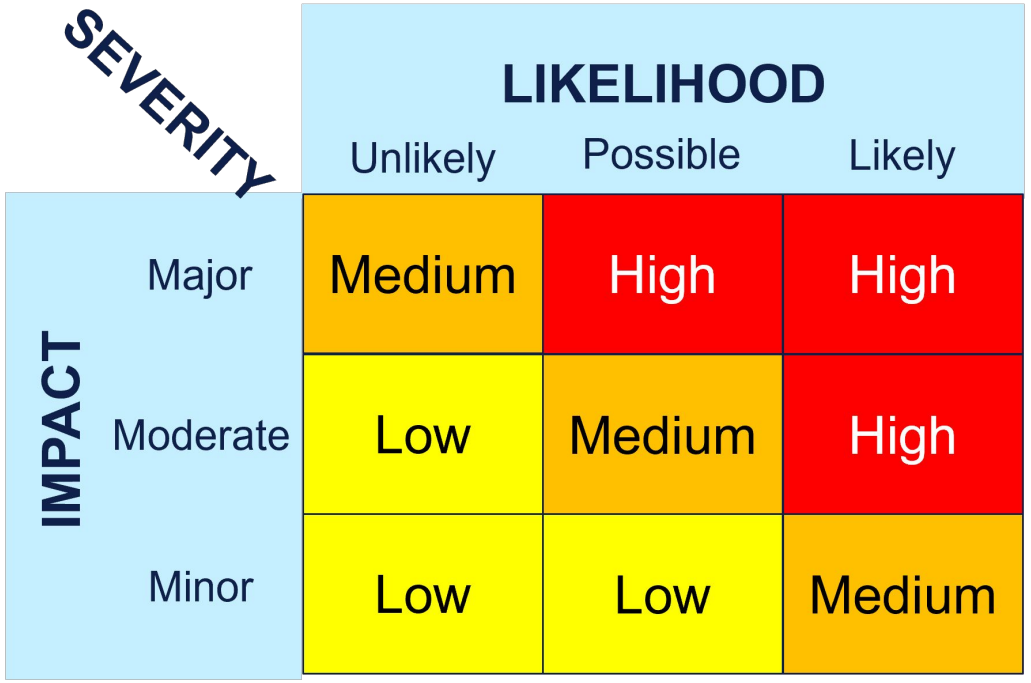
  XÁC SUẤT x TÁC ĐỘNG = MỨC ĐỘ NGHIÊM TRỌNG

- Mỗi tham số phải được xác định lại để phù hợp với bối cảnh an ninh mạng
- Ví dụ:

xác suất ~ dễ truy cập, dễ khai thác, có sẵn mã khai thác

tác động ~ thỏa hiệp về phạm vi

mức độ nghiêm trọng ~ vấn đề an toàn, vi phạm quy định, chế tài / chi phí bổ sung



DNV

Ví dụ về định nghĩa ma trận rủi ro

Ảnh hưởng đối với giá trị công ty							Xác suất xảy ra				
	Quy định và tuân thủ	**An toàn**	**An ninh và chất lượng cung cấp**	**Tài chính**	**Hình ảnh với công chúng**	**Tính bền vững**	**Hiếm khi** *dưới 1 lần trong 100 năm*	**Ít khả năng** *dưới 1 lần trong 10 năm*	**Đôi khi** *dưới 1 lần mỗi năm*	**Thường xuyên** *1-10 lần mỗi năm*	**Rất thường xuyên** *Hơn 10 lần mỗi năm*
Thảm họa	*Xung đột cơ cấu với cơ quan chức năng, thu hồi giấy phép, tiền phạt luỹ kế, có khả năng bị phạt tù*	*Nhiều trường hợp tử vong*	*>10 triệu phút mất điện*	*Thiệt hại >€10 triệu*	*Các vụ việc bị công chúng biết đến rộng rãi, trong thời gian dài*	*Phát thải CO_2 >500 nghìn tấn*					
Nghiêm trọng	*Thỉnh thoảng xung đột với cơ quan chức năng. phạt hành chính hoặc khởi tố hình sự với hội đồng quản trị*	*Các vụ tai nạn dẫn đến tử vong hoặc thương tích rất nghiêm trọng*	*1-10 triệu phút mất điện*	*Thiệt hại € 1-10 triệu*	*Các vụ việc bị công chúng biết đến rộng rãi, trong thời gian ngắn*	*Phát thải CO_2 50-500 nghìn tấn*					
Đáng kể	*Nộp phạt, khởi kiện thay mặt cho hơn 5.000 khách hàng, vướng mắc với cơ quan chức năng*	*Các vụ tai nạn gây thương tích nghiêm trọng và có sự vắng mặt*	*100 nghìn -1 triệu phút mất điện*	*Thiệt hại €100 nghìn -1 triệu*	*Các vụ việc bị công chúng biết đến trong phạm vi nhỏ, trong thời gian dài*	*Phát thải CO_2 5-50 nghìn tấn*					
Nhỏ	*Chỉ định bắt buộc, khởi kiện thay mặt hơn 500 khách hàng, thỉnh thoảng có vướng mắc với cơ quan chức năng*	*Tai nạn gây thương tích và có sự vắng mặt*	*10-100 nghìn phút mất điện*	*Thiệt hại €10.000-100.000*	*Các vụ việc bị công chúng biết đến trong phạm vi nhỏ, trong thời gian ngắn*	*Phát thải CO_2 0,5-5 nghìn tấn*					
Không đáng kể	*Cảnh cáo, khởi kiện hơn 50 khách hàng, bất đồng với cơ quan chức năng*	*Suýt xảy ra tai nạn hoặc thương tích nhẹ nhưng không có sự vắng mặt*	*<10 nghìn phút mất điện*	*Thiệt hại <€10.000*	*Các vụ việc không bị công chúng biết đến*	*Phát thải CO_2 <0,5 nghìn tấn*					

Xác suất có thể được định lượng theo nhiều cách khác nhau

$$Mối\ nguy * Lỗ\ hổng \mid \frac{Mối\ nguy * Lỗ\ hổng}{Khả\ năng\ phục\ hồi} \mid sử\ dụng\ thông\ số \mid Kinh\ nghiệm\ và\ phán\ đoán$$

Nhận dạng rủi ro

Công thức cần nhớ



Rủi ro nằm ở đâu?



Con người

- Đào tạo và nhận thức?
- Kỹ năng và trình độ chuyên môn?
- Diễn tập tình huống khẩn cấp?
- Cấp quyền và xác thực?
- An ninh vật lý?





Công nghệ

- Thiết kế hệ thống và mạng?
- Bảo vệ điểm cuối?
- Cấu hình phần mềm?
- Giao thức mã hóa?
- Phát hiện và giám sát?



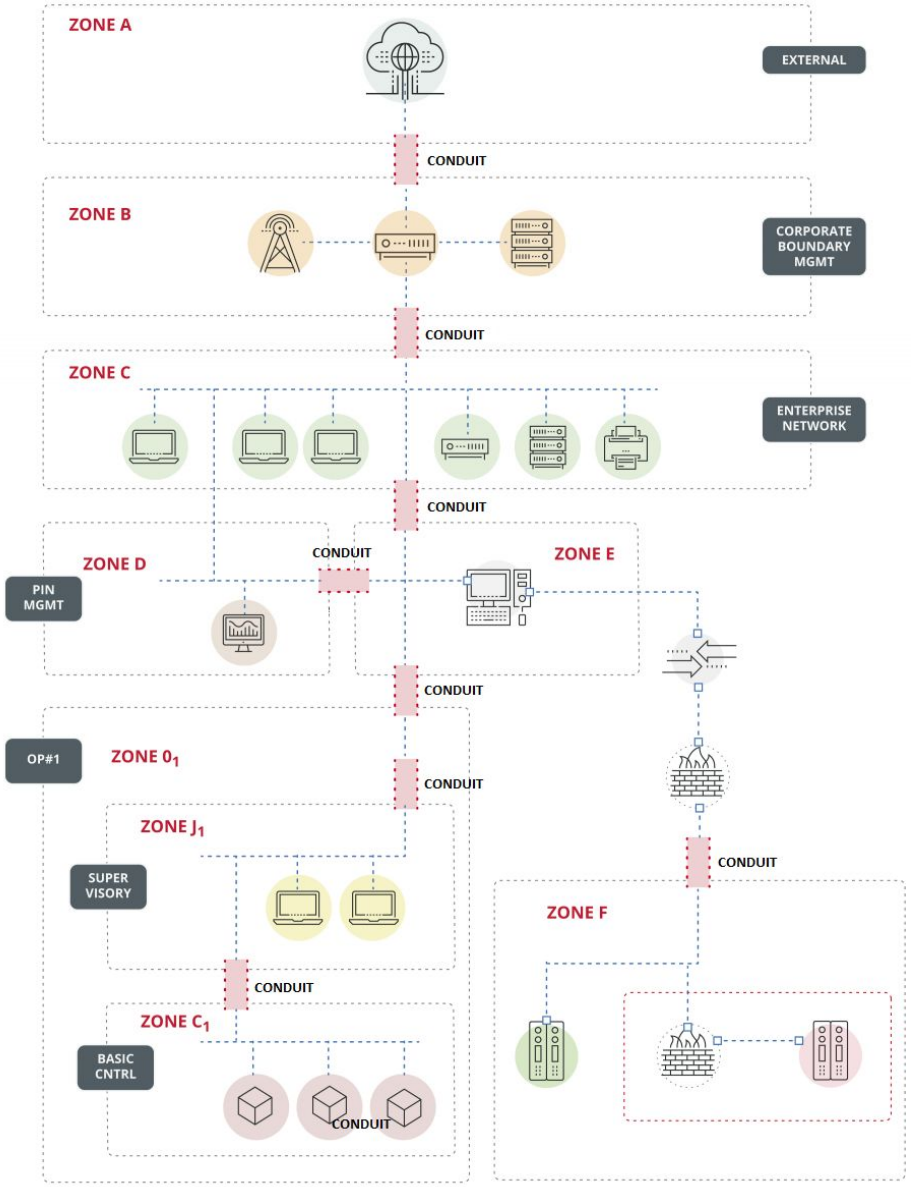
Kiểm kê tài sản

- Kiểm kê tài sản nhằm mục tiêu duy trì thông tin trên tất cả các thiết bị, cấu phần phần cứng, cấu phần phần mềm và giao thức/cổng giao tiếp:
  - Tổ chức chịu trách nhiệm
  - Nhà sản xuất, nhà cung cấp, model, phiên bản, số sê-ri
  - Hệ điều hành
  - Mức độ sửa đổi / vá lỗi
  - Địa chỉ mạng (cổng vật lý, địa chỉ IP)
  - Lịch sử

- Thông tin kiểm kê tài sản phải được cập nhật thường xuyên để phản ánh tình trạng mới nhất
  - Cập nhật khi có thay đổi trong hệ thống (nâng cấp, ngừng hoạt động, cài đặt mới, vá lỗi)
  - Rà soát định kỳ, ngay cả trong trường hợp không có thay đổi

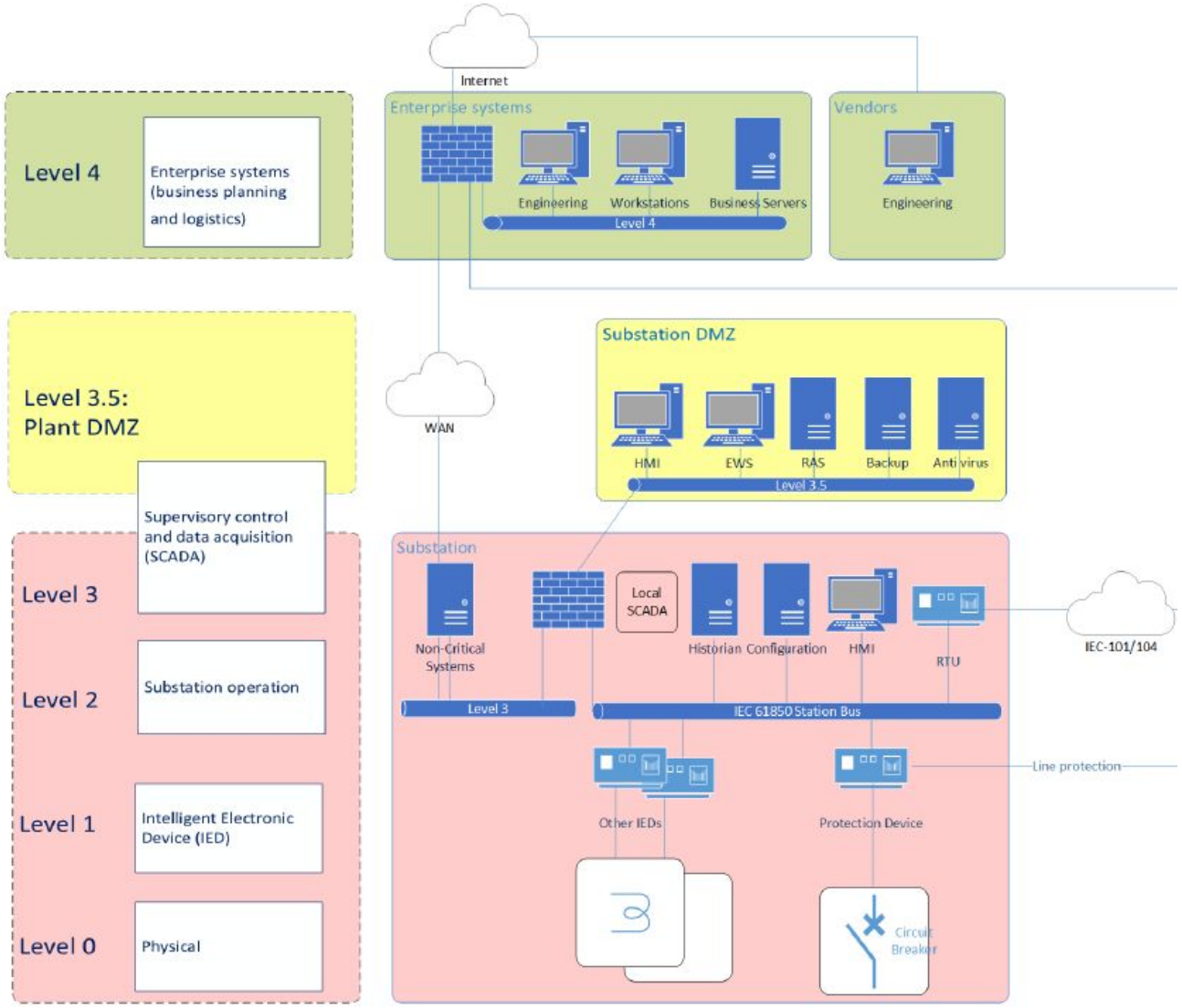
Kiến trúc hệ thống

- Kiến trúc hệ thống thể hiện cách thức các thiết bị được kết nối vật lý tại địa điểm
  - Bộ biến đổi nguồn
  - Bộ điều khiển sơ cấp (ví dụ BCU, rơle bảo vệ, RTU)
  - Bộ điều khiển thứ cấp (Bộ điều khiển SAS, cổng trạm biến áp)
  - Máy chủ (HMI, máy trạm kỹ thuật, Historian, máy chủ SCADA, FEP, màn hình treo tường)
  - Thiết bị mạng (switch, router, tường lửa)
- Thiết bị ảo phải được xử lý giống như máy chủ vật lý



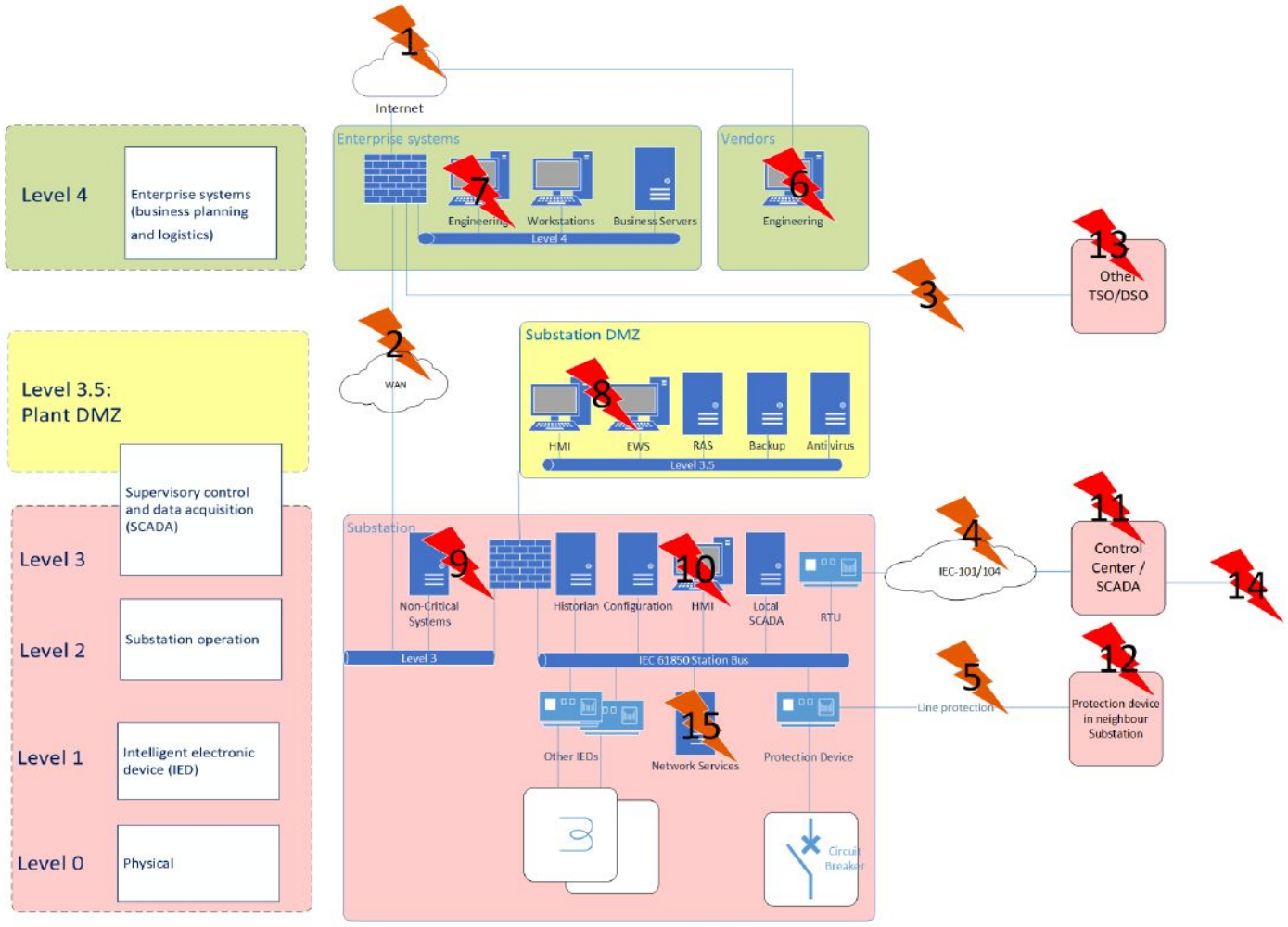
Sơ đồ luồng dữ liệu

- Luồng dữ liệu thể hiện cách trao đổi thông tin trong hệ thống
  - Nút nguồn
  - Nút chìm
  - Nút trung gian
  - Tuyến (có dây và không dây)
  - Giao thức ứng dụng (http, https, ftp, NTP, PTP, SSH, MODBUS, DNP3.0)
- Mô hình Purdue thường được sử dụng để thể hiện cách truyền dữ liệu từ cấp trường dữ liệu đến doanh nghiệp và ngược lại



DNV ©

Lập mô hình mối nguy để hiểu rõ cuộc tấn công liên quan



- Tấn công từ internet (1)
- Tấn công từ mạng nội bộ (2, 3, 4, 14)
- Tấn công từ mạng chuyển tiếp liên phân vùng (5)
- Tấn công từ truy cập từ xa (6, 13)
- Tấn công qua hệ thống nội bộ (7, 8, 9, 10, 11, 12

Đánh giá rủi ro

DNV ©

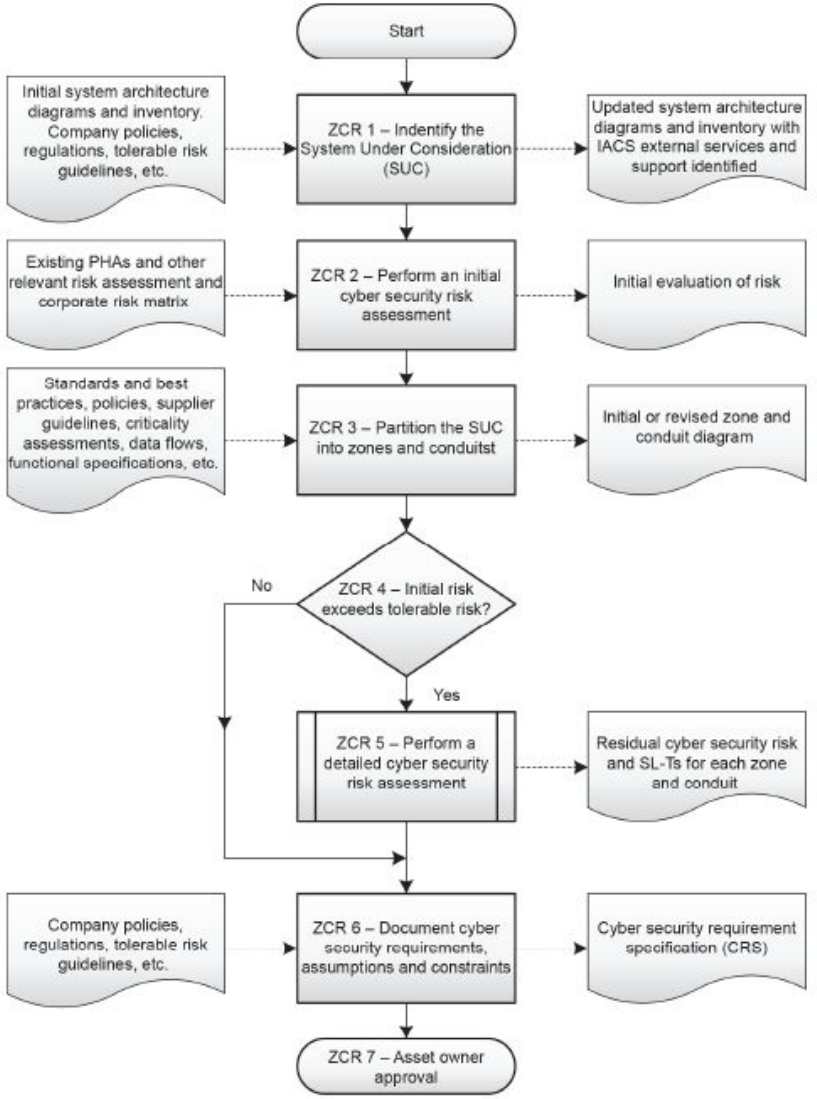
Đánh giá rủi ro (IEC 62443)

Tìm hiểu
Hệ thống đang xem xét

Đánh giá tổng quát
Xác định các khu vực và đường dẫn / Mục tiêu cấp độ an ninh (mức độ quan trọng), Tài sản, Dễ truy cập

Đánh giá chi tiết
Xác định và đánh giá các nguy cơ, sự kiện, hậu quả, rào cản, Xác định và đánh giá các rào cản bổ sung cần thiết để đạt được mục tiêu (SL-T)

Đánh giá & Báo cáo



Các cấp độ an ninh

Tham khảo: Hướng dẫn bắt đầu ISAGCA: Tổng quan về tiêu chuẩn ISA/IEC 62443

- Thước đo độ tin cậy để đảm bảo rằng hệ thống, phân vùng hoặc các kênh thông tin không có lỗ hổng và hoạt động như dự kiến.
- Yêu cầu kỹ thuật
- Được xác định dưới dạng phương tiện, nguồn lực, kỹ năng, yếu tố thúc đẩy

- Các loại:
  1. SL-C = năng lực tự nhiên
  2. SL-T = mục tiêu
  3. SL-A = đạt được

Security Level	Definition	Means	Resources	Skills	Motivation
1	Protection against casual or coincidental violation	simple	low	generic	low
2	Protection against intentional violation using simple means with low resources, generic skills, and low motivation				
3	Protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation	sophisticated	moderate	IACS-specific	moderate
4	Protection against intentional violation using sophisticated means with extended resources, IACS-specific skills, and high motivation	sophisticated	extended	IACS-specific	high

Đánh giá tổng quát

- Cách tiếp cận từ trên xuống
- Xác định
  - phân vùng và các kênh thông tin
  - Mục tiêu cấp độ an ninh (mức độ quan trọng, SL-T)
  - Tài sản
  - Dễ dàng tiếp cận

Đánh giá chi tiết

- Cách tiếp cận từ dưới lên
- Nhận diện và đánh giá:
  - Nguy cơ, sự kiện, hậu quả,
  - Rào cản
  - Các rào cản bổ sung cần thiết để đạt được mục tiêu (SL-T)

Cấp độ an ninh đạt được (SL-A) ít nhất phải bằng Mục tiêu cấp độ an ninh (SL-T)

Khoảng trống cần được loại bỏ bằng các biện pháp kiểm soát bổ sung

DNV

Quy trình đánh giá rủi ro bắt đầu bằng việc xác định các cuộc tấn công liên quan

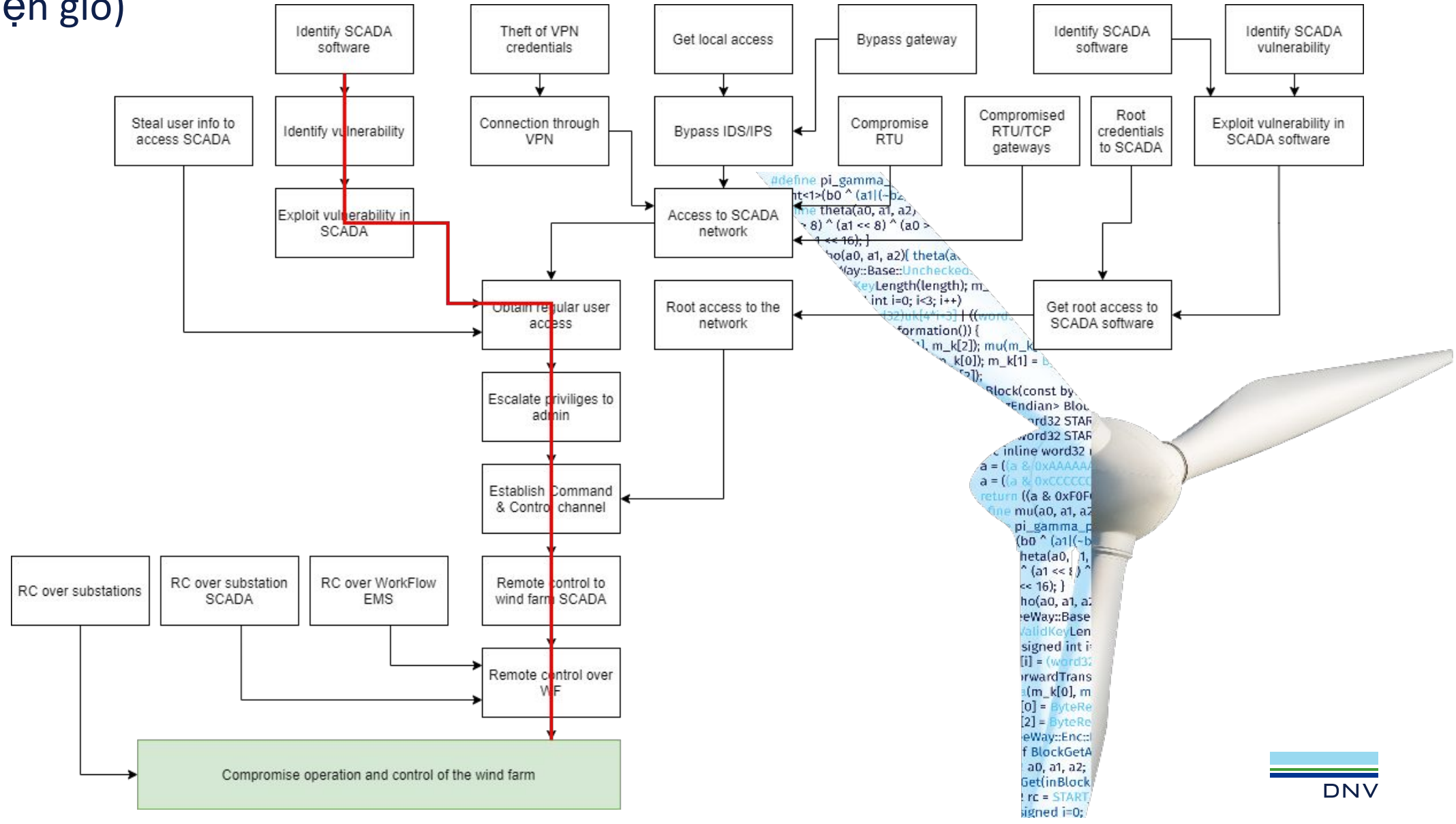
Các cuộc tấn công đến từ nhiều nguồn khác nhau

- Tài sản vật lý (trạm biến áp)
- Internet công cộng
- Mạng bên ngoài
- Mạng nội bộ

Các nguy cơ điển hình được xem xét

- Tái sử dụng thông tin xác thực
- Thông tin xác thực mặc định/yếu
- Tấn công từ chối dịch vụ
- Khai thác kiến trúc mạng yếu
- Khai thác cấu hình hạn chế của các giao thức an ninh
- Khai thác lỗ hổng hệ thống
- Đưa dữ liệu/thông tin sai
- Lừa đảo
- Phần mềm độc hại
- …

Phân tích chi tiết một cuộc tấn công
(Nhà máy điện gió)



Bước 1: Đánh giá rủi ro ban đầu về các nguy cơ và kịch bản khác nhau

Attacks comming from the Substations								
Threats	**Scenario description**	**Probability**	**Impact**	**Risk**	**Security measures**	**Res. Prob.**	**Res. Impact**	**Res. Risk**
Credential Reuse	This includes for example using one password for a group of people (e.g. for the field engineers). When credentials are reused between a group of people, it will be unclear which user performed an action within the substation Remark: We only consider authorized users here.	Very Often	Substantial		**C.1.1.1, C.1.1.3, C.1.1.4**, C.1.1.5	Unlikely	Substantial	
Default/weak credentials	This also includes using no credentials at all. If default/weak or no credentials are used, it will be relatively easy for authorized **or unauthorized persons** to execute certain attacks from within the substation. This potentially allows them to damage the systems, trying to hack the SCADA/EMS system from withing the substation, trying to remotely access other substations and hack into these substations, try to perform switching actions locally.	Often	Serious		**C.1.1.3**, C.1.1.5, **C.1.1.6**	Unlikely	Serious	
Privilege escalation	A field engineer is able to increase his privileges on the components locally in the substation and case damage there (e.g. unauthorized switching actions, reconfiguration of RTUs, IEDs, ...) Remark: Here we only include the scenario where an authorized persons increases his access rights into systems, components, ...	Sometimes	Substantial		**C.1.1.1, C.1.2.1**	Unlikely	Substantial	
Denial of Service attacks	An authorized/unauthorized person, physically accessing the substations, tries to launch a denial of service attack towards the SCADA/EMS system or towards the other substations. This may cause the SCADA/EMS system to stop functioning correctly or other substation RTUs to stop working. (MAC address security / unused ports are closed)	Unlikely	Serious		**B.1.5.4, B.1.5.10, B.1.6.1, B.1.6.2, C.1.3.2, C.1.3.3, C.1.3.6, C.1.3.7, C.1.3.8**	Unlikely	Substantial	

Bước 2: Các biện pháp an ninh được bổ sung để giảm thiểu nguy cơ và các kịch bản khác nhau

Attacks comming from the Substations								
Threats	**Scenario description**	**Probability**	**Impact**	**Risk**	**Security measures**	**Res. Prob.**	**Res. Impact**	**Res. Risk**
Credential Reuse	This includes for example using one password for a group of people (e.g. for the field engineers). When credentials are reused between a group of people, it will be unclear which user performed an action within the substation Remark: We only consider authorized users here.	Very Often	Substantial		**C.1.1.1, C.1.1.3, C.1.1.4**, C.1.1.5	Unlikely	Substantial	
Default/weak credentials	This also includes using no credentials at all. If default/weak or no credentials are used, it will be relatively easy for authorized **or unauthorized persons** to execute certain attacks from within the substation. This potentially allows them to damage the systems, trying to hack the SCADA/EMS system from withing the substation, trying to remotely access other substations and hack into these substations, try to perform switching actions locally.	Often	Serious		**C.1.1.3**, C.1.1.5, **C.1.1.6**	Unlikely	Serious	
Privilege escalation	A field engineer is able to increase his privileges on the components locally in the substation and case damage there (e.g. unauthorized switching actions, reconfiguration of RTUs, IEDs, ...) Remark: Here we only include the scenario where an authorized persons increases his access rights into systems, components, ...	Sometimes	Substantial		**C.1.1.1, C.1.2.1**	Unlikely	Substantial	
Denial of Service attacks	An authorized/unauthorized person, physically accessing the substations, tries to launch a denial of service attack towards the SCADA/EMS system or towards the other substations. This may cause the SCADA/EMS system to stop functioning correctly or other substation RTUs to stop working. (MAC address security / unused ports are closed)	Unlikely	Serious		**B.1.5.4, B.1.5.10, B.1.6.1, B.1.6.2, C.1.3.2, C.1.3.3, C.1.3.6, C.1.3.7, C.1.3.8**	Unlikely	Substantial	

Bước 3: Ước tính rủi ro còn lại (kết hợp giữa xác suất còn lại và tác động)

Attacks comming from the Substations								
Threats	**Scenario description**	**Probability**	**Impact**	**Risk**	**Security measures**	**Res. Prob.**	**Res. Impact**	**Res. Risk**
Credential Reuse	This includes for example using one password for a group of people (e.g. for the field engineers). When credentials are reused between a group of people, it will be unclear which user performed an action within the substation Remark: We only consider authorized users here.	Very Often	Substantial		**C.1.1.1, C.1.1.3, C.1.1.4**, C.1.1.5	Unlikely	Substantial	
Default/weak credentials	This also includes using no credentials at all. If default/weak or no credentials are used, it will be relatively easy for authorized **or unauthorized persons** to execute certain attacks from within the substation. This potentially allows them to damage the systems, trying to hack the SCADA/EMS system from withing the substation, trying to remotely access other substations and hack into these substations, try to perform switching actions locally.	Often	Serious		**C.1.1.3**, C.1.1.5, **C.1.1.6**	Unlikely	Serious	
Privilege escalation	A field engineer is able to increase his privileges on the components locally in the substation and case damage there (e.g. unauthorized switching actions, reconfiguration of RTUs, IEDs, ...) Remark: Here we only include the scenario where an authorized persons increases his access rights into systems, components, ...	Sometimes	Substantial		**C.1.1.1, C.1.2.1**	Unlikely	Substantial	
Denial of Service attacks	An authorized/unauthorized person, physically accessing the substations, tries to launch a denial of service attack towards the SCADA/EMS system or towards the other substations. This may cause the SCADA/EMS system to stop functioning correctly or other substation RTUs to stop working. (MAC address security / unused ports are closed)	Unlikely	Serious		**B.1.5.4, B.1.5.10, B.1.6.1, B.1.6.2, C.1.3.2, C.1.3.3, C.1.3.6, C.1.3.7, C.1.3.8**	Unlikely	Substantial	

Kiểm soát an ninh và xác định ưu tiên rủi ro

DNV ©

Từ đánh giá rủi ro đến chiến lược an ninh

- Đánh giá rủi ro xác định các mối nguy và rủi ro không thể chấp nhận được
- Các biện pháp kiểm soát và giảm nhẹ mối nguy về an ninh mạng cần thiết (bao gồm các biện pháp kiểm soát dựa trên kỹ thuật) được xác định
- Các biện pháp kiểm soát và giảm nhẹ được bao gồm trong các chính sách và quy trình an ninh
- Thực hiện kiểm toán để thẩm định quy trình và hiệu quả của các biện pháp kiểm soát



DNV ©

Đánh giá rủi ro hình nơ (bow tie)



- Rào cản kiểm soát làm giảm khả năng xảy ra sự kiện hàng đầu có thể gây ra hậu quả.
- Rào cản khôi phục làm giảm mức độ nghiêm trọng của hậu quả.
- Yếu tố leo thang là các tình huống, điều kiện hoặc hoàn cảnh có thể dẫn đến sự thất bại một phần hoặc toàn bộ rào cản.

DNV ©

Ví dụ về kiểm soát an ninh



Con người

- Đào tạo nâng cao nhận thức
- Mô phỏng về hành vi giả mạo
- Bài tập trên bàn
- Kiểm tra lý lịch của nhân viên có quyền truy cập đặc quyền



Quy trình

- Đánh giá an ninh
- Yêu cầu mua sắm
- Các yêu cầu về ghi nhận thông tin
- Kiểm soát truy cập dựa trên vai trò



Công nghệ

- ID/IPS
- Mã hóa
- Tăng cường hệ thống
- Phân đoạn mạng

Nguồn tham khảo các biện pháp kiểm soát được đề xuất: NIST SP 800-53 | ISO 27002 và 27019 | IEC 62443 3-1

Lưu ý: Giải pháp kỹ thuật và hệ thống an toàn cũng có thể là biện pháp kiểm soát an ninh

DNV ©

Phát hiện	Định nghĩa
Không bị phát hiện (5)	Có thể phát hiện và xác minh lỗi bằng cách quan sát trong thời gian dài (hơn 6 tháng).
Thấp (4)	Lỗi chỉ có thể được phát hiện và xác minh khi áp dụng lịch bảo trì định kỳ (3 tháng hoặc 6 tháng).
Trung bình (3)	Lỗi có thể được phát hiện và xác minh trong vài ngày
Cao (2)	Lỗi có thể được phát hiện và xác minh trong vài giờ.
Chắc chắn (1)	Lỗi có thể được phát hiện và xác minh ngay lập tức.

FMEA RPN

- Phân tích phương thức lỗi và tác động
- Số ưu tiên rủi ro

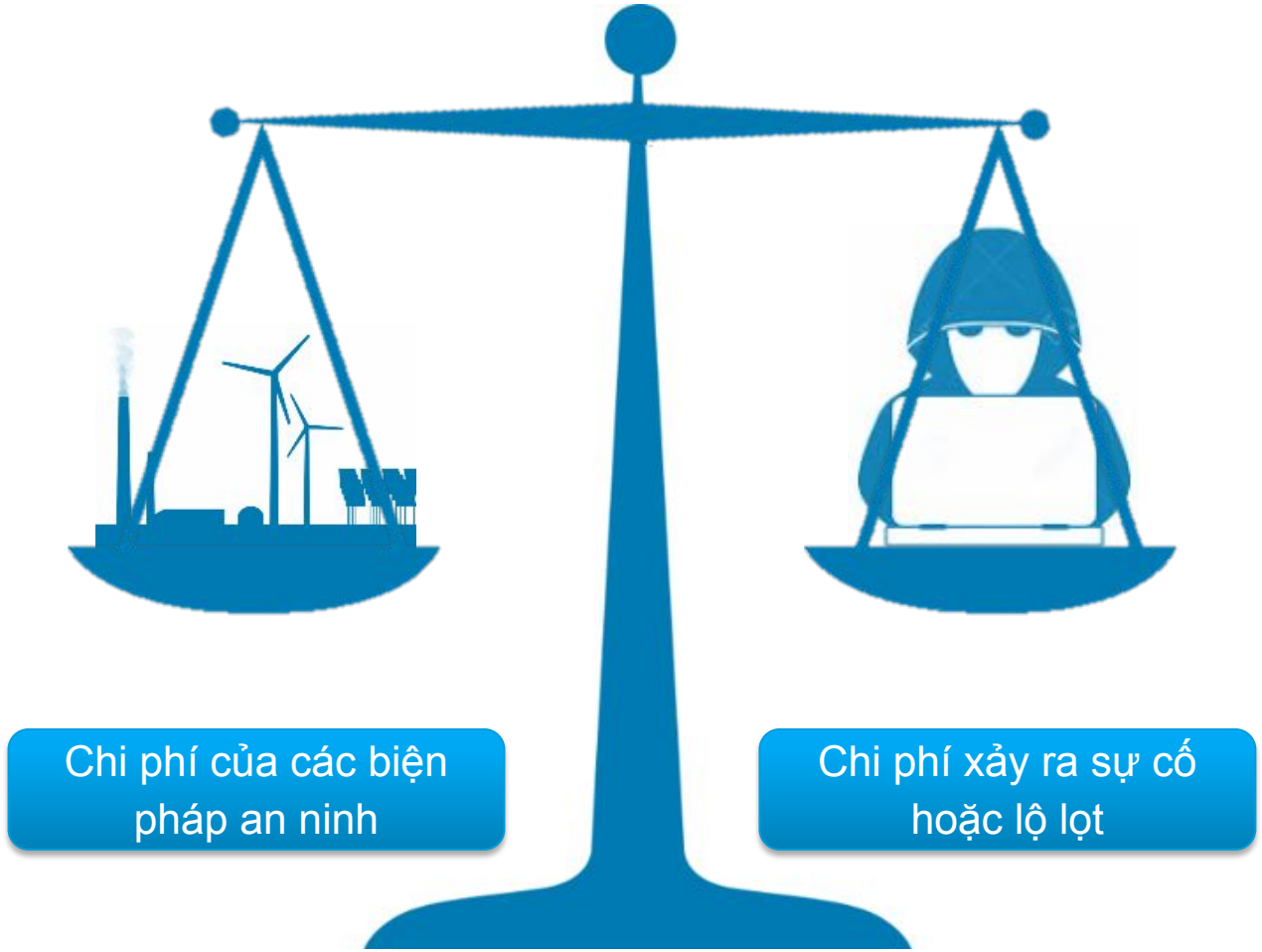
RPN = MỨC ĐỘ NGHIÊM TRỌNG * PHÁT HIỆN

- Khả năng phát hiện lỗi được đánh giá theo thang điểm
  - Xếp hạng về sự phát hiện ở mức cao thể hiện khả năng phát hiện thấp
- Tổ chức nên ưu tiên những rủi ro không thể chấp nhận được với khả năng phát hiện thấp

DNV

Không thể đảm bảo an ninh 100%

Khả năng quản lý rủi ro an ninh là yếu tố then chốt!



Chi phí của các biện pháp an ninh

Chi phí xảy ra sự cố hoặc lộ lọt

Yêu cầu về quản trị – Chính sách, Tiêu chuẩn, Hướng dẫn, Quy trình

- *CIIO phải thiết lập và thực hiện các chính sách, tiêu chuẩn, hướng dẫn và quy trình*
- *Phải được rà soát ít nhất 12 tháng/lần*
- *Phải đảm bảo tính nhất quán giữa thực tiễn và việc triển khai*



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Yêu cầu về quản trị – Chính sách

- *Quản lý cấp cao CIP phải rà soát và phê duyệt các chính sách an ninh mạng ít nhất 15 tháng/lần*
- *Kế hoạch an ninh mạng bằng văn bản phải được triển khai cho Hệ thống an ninh mạng của BES tác động thấp*
- *Quản lý cấp cao CIP phải được xác định theo tên và mọi thay đổi phải được ghi lại trong vòng 30 ngày dương lịch kể từ ngày thay đổi*
- *Việc ủy quyền phải được thực hiện theo quy trình đã lập thành văn bản*

- CIP-003-8



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DNV

Yêu cầu về quản trị – Lồng ghép an ninh mạng từ thiết kế

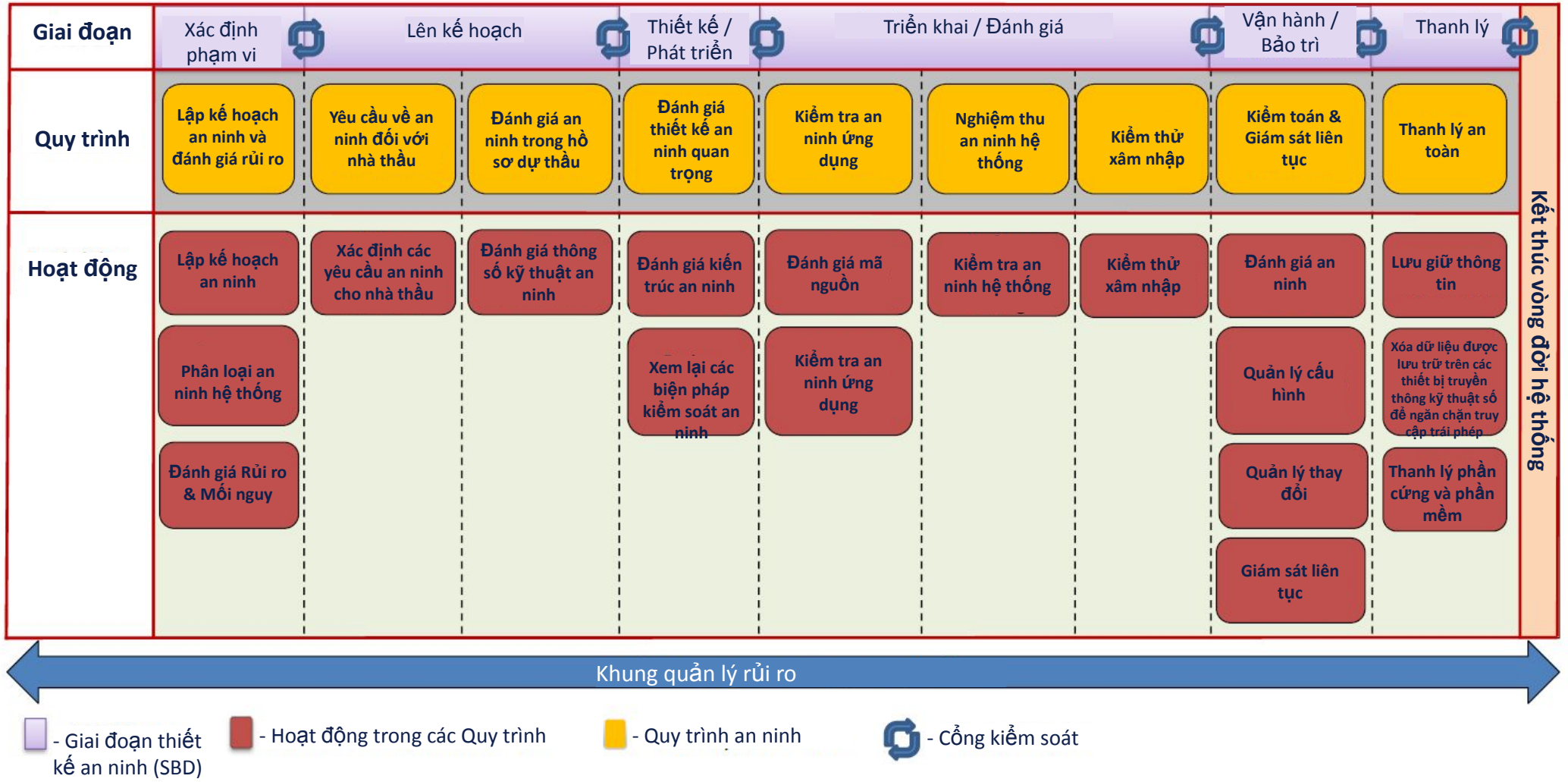
- CIIO phải áp dụng bảo mật theo khung thiết kế do CSA thiết lập
- Tất cả các phần không áp dụng đều phải được ghi lại bằng văn bản với lý do chính đáng.



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Lồng ghép an ninh mạng từ thiết kế



Thế nào là Đảm bảo an ninh từ khâu thiết kế?

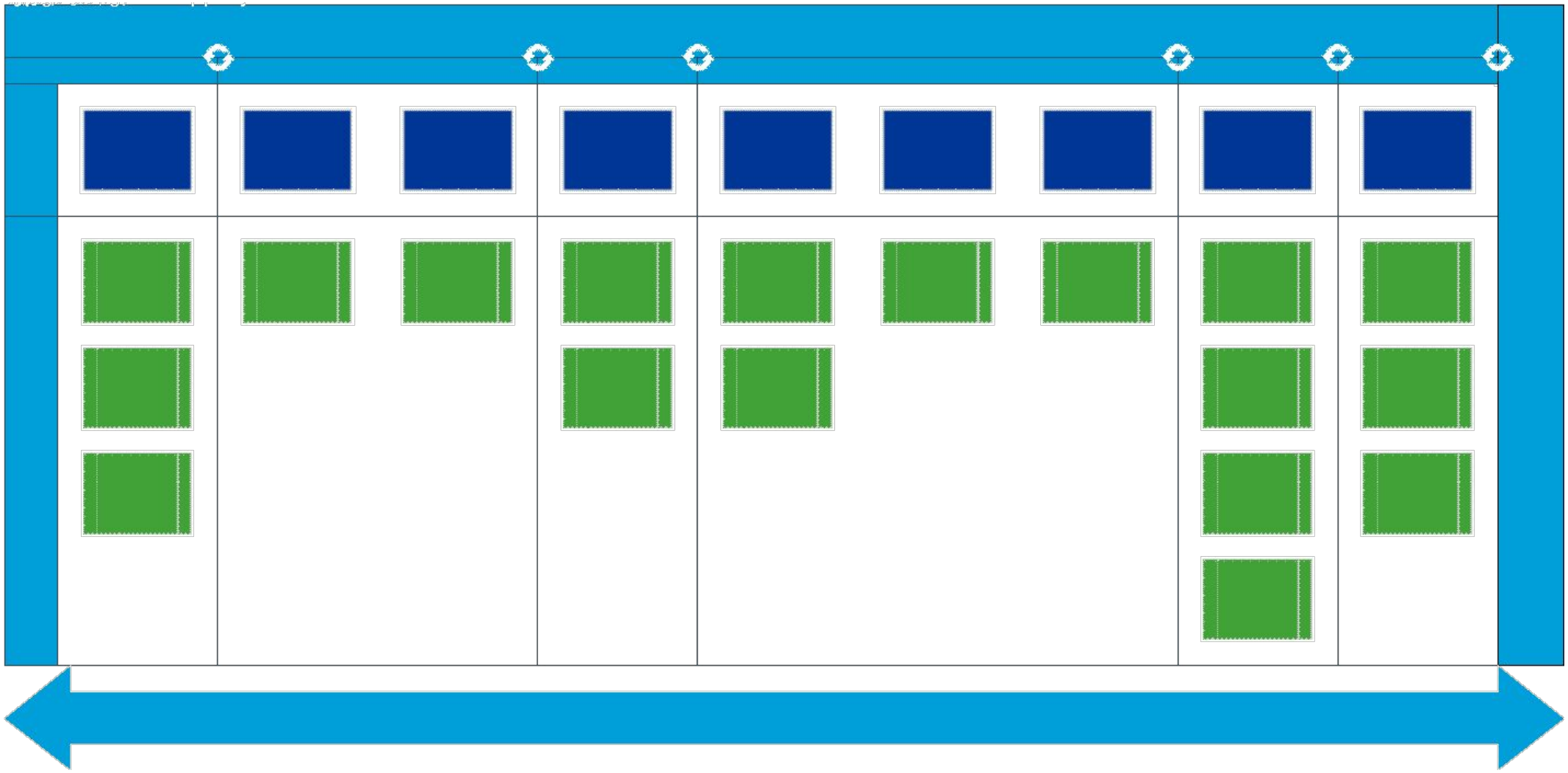
DNV ©

Đảm bảo an ninh từ khâu thiết kế

“ **Đảm bảo an ninh từ khâu thiết kế** ” là thuật ngữ để chuyển những cân nhắc về an ninh mạng từ người dùng cuối của hệ thống sang các kỹ sư của hệ thống. Để giảm khối lượng công việc của người dùng cuối trong việc giải quyết vấn đề an ninh trong giai đoạn vận hành hệ thống, ***các quyết định về an ninh cần được đưa ra trong quá trình làm kỹ thuật công trình/thiết bị*** và theo cách mà các bên thứ ba có thể theo dõi được.

- Fluchs S, Taştan E, Trumpf T, Horch A, Drath R, Fay A. Các quyết định về Đảm bảo an ninh từ khâu thiết kế có thể theo dõi cho các hệ thống vật lý điện tử (CPS) bằng các sơ đồ dựa trên chức năng và Thư viện an ninh. *Cảm biến* . 2023; 23(12):5547. https://doi.org/10.3390/s23125547

Lồng ghép Đảm bảo an ninh vào thiết kế

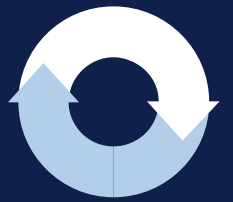


Được lựa chọn theo hướng đảm bảo an ninh theo nguyên tắc thiết kế

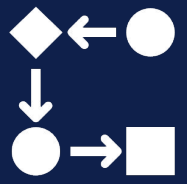
Phòng thủ chuyên sâu



Dù Hỏng lỗi vẫn an toàn



Đặc quyền ở mức tối thiểu nhất



Chống thoái thác



Kỹ thuật công trình dựa trên yêu cầu về an ninh mạng



DNV ©

Phòng thủ chuyên sâu

Phòng thủ chuyên sâu (DiD)

- Mỗi biện pháp an ninh là một trở ngại
- Trở ngại có thể bị đánh bại
- Làm chậm bước tiến của kẻ tấn công
- Tạo cơ hội để phát hiện và giảm nhẹ



Các biện pháp kiểm soát có thể bị qua mặt

Ngày 0

Lỗ hổng chưa được vá

Thông tin truy cập/xác thực bị xâm phạm

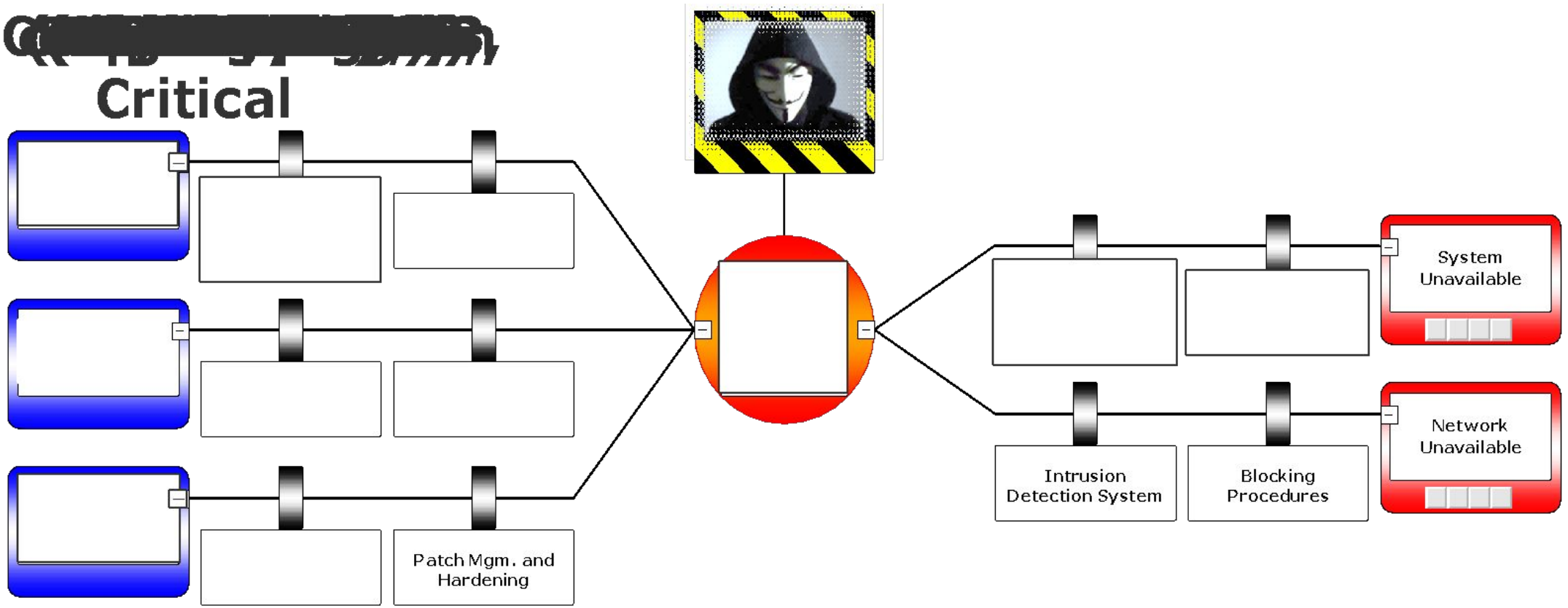
Mối đe dọa từ kẻ tay trong

Cấu hình kém

Các kỹ thuật né tránh

DNV ©

Ví dụ về kiểm soát an ninh phân lớp



DNV ©

Dù hỏng lỗi vẫn an toàn (Thất bại một cách an toàn)

Thế nào là Hỏng lỗi vẫn đảm bảo an ninh?

Hỏng lỗi vẫn an toàn nghĩa là triển khai logic quyết định để **đưa hệ thống vào trạng thái an ninh an toàn khi xảy ra lỗi** . Việc xử lý lỗi một cách an toàn sẽ đảm bảo rằng đường dẫn lỗi, chẳng hạn như các trường hợp ngoại lệ, không làm lộ thông tin bổ sung mà lẽ ra bình thường không bị lộ.

- Lực lượng bán hàng

Làm thế nào để Hỏng lỗi vẫn an toàn trong hệ thống OT?

Hoạt động đảo



- Là một hệ thống được thiết kế theo cách có thể hoạt động độc lập và tách biệt với các hệ thống khác
- Chế độ vận hành đảo có thể được kích hoạt như một biện pháp Xử lý sự cố

Dự phòng



- Hệ thống nào cũng cần có dự phòng ở mọi cấp độ
- Phải có khả năng chống chịu cao trước các lỗi ở các hệ thống con
- Thiết lập hệ thống dự phòng thông qua quá trình đánh giá rủi ro

Hỏng lỗi vẫn an toàn



- IED và RTU cấp 1 có thể hoạt động độc lập trong một khoảng thời gian sau khi ngắt kết nối với máy chủ SCADA
- IED và RTU cấp 1 được cấu hình để khắc phục các sự cố nhỏ và có thể dự đoán được độc lập với máy chủ SCADA

Đặc quyền ở mức tối thiểu

DNV ©

Đặc quyền ở mức tối thiểu là gì?

Nguyên tắc *Đặc quyền ở mức tối thiểu* vận hành bằng cách giới hạn chỉ cho phép truy cập dữ liệu, tài nguyên, ứng dụng và chức năng ứng dụng ở mức mà người dùng hoặc một đơn vị nào đó cần để thực hiện nhiệm vụ hoặc quy trình công việc cụ thể của họ.

-Mạng Palo Alto

Làm thế nào để thực thi Đặc quyền ở mức tối thiểu ?

“Việc kiểm tra quyền thường xuyên, còn được gọi là đánh giá quyền truy cập của người dùng, giúp các tổ chức xác định các quyền không cần thiết và ngăn chặn quyền truy cập không mong muốn vào dữ liệu nhạy cảm.”

- Tenfold Security (An ninh gấp 10 lần)

Kiểm soát truy cập dựa trên vai trò (RBAC)



- Nguyên tắc về cấp quyền
- Mỗi vai trò được cấp số lượng quyền tối thiểu cần thiết cho vai trò đó
- Đơn giản hóa việc thực hiện Đặc quyền ở mức tối thiểu
- Cân nhắc khi thiết lập người dùng và quyền trên AD

Phân đoạn mạng



- Mô hình Perdue
- Đảm bảo rằng phần tử hệ thống chỉ có thể giao tiếp với các phần tử cần thiết trong hệ thống
- Được thực thi bằng các Bộ chuyển mạch (VLAN), Tường lửa và Bộ định tuyến

Chống thoái thác

Chống thoái thác là gì?

Là biện pháp bảo vệ chống lại tình trạng một cá nhân phủ nhận một cách sai sự thật việc đã thực hiện một hành động nhất định và cung cấp khả năng xác định xem một cá nhân có thực hiện một hành động nhất định hay không, chẳng hạn như tạo thông tin, gửi tin nhắn, phê duyệt thông tin hoặc nhận tin nhắn.

NIST.SP.800-53r5

Làm thế nào để đảm bảo tính năng Chống thoái thác?

“Các biện pháp kiểm soát Chống thoái thác đóng vai trò là trụ cột chính của pháp y kĩ thuật số (= điều tra sau sự cố trên môi trường số), cung cấp một lá chắn đáng gờm chống lại sự xói mòn tính toàn vẹn của bằng chứng và trách nhiệm giải trình.”

Chữ ký số



- 3 loại: SES, AES, & QES
- HMAC và Hash có khóa bí mật cũng có thể được sử dụng làm chữ ký số

Tài khoản cá nhân



- Tài khoản riêng biệt cho mọi người dùng
- Tài khoản riêng biệt cho mọi dịch vụ
- Không có tài khoản chia sẻ ở bất cứ đâu
- Không chia sẻ mật khẩu

Đồng bộ hóa thời gian



- Đảm bảo rằng dấu thời gian trên nhật ký có tính xác tín
- Đồng hồ GPS với Giao thức thời gian mạng
- Đồng bộ hóa đến vài mili giây

Bên thứ ba đáng tin cậy



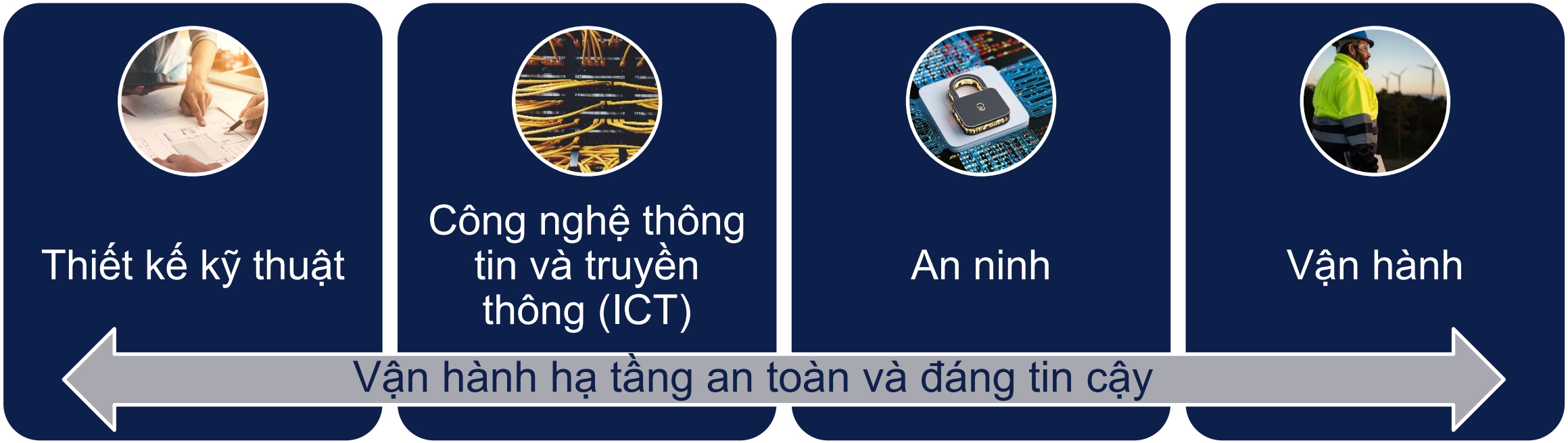
- Cơ sở hạ tầng khóa công khai (PKI) trong các hệ thống Air-Gapped
- Bổ sung thực hiện chữ ký số

Kỹ thuật công trình dựa trên yêu cầu về an ninh mạng

DNV ©

DNV

Các phòng ban hoạt động độc lập (silos) trong tổ chức với mục tiêu chung



Kỹ thuật công trình dựa trên yêu cầu về an ninh mạng (**CIE**) là một phương pháp mới nổi để tích hợp các cân nhắc về an ninh mạng vào ý tưởng, thiết kế, phát triển và vận hành của bất kỳ hệ thống vật lý, năng lượng nào hoặc mặt khác, nhằm giảm thiểu hoặc thậm chí loại bỏ các con đường cho các cuộc tấn công mạng.

-Văn phòng An ninh mạng, An ninh Năng lượng và Ứng phó Khẩn cấp - Bộ Năng lượng Hoa Kỳ

Tấn công vật lý mạng

Ukraina 2015



- Các bộ ngắt mạch bị mở từ xa với thông tin xác thực của cán bộ vận hành bị xâm phạm
- Thiết bị CNTT bị xóa
- điện được phục hồi thủ công trong vòng vài giờ

Ukraina 2016



- vận hành bộ ngắt mạch từ xa bằng cách phát lại các thông báo lệnh
- Từ chối dịch vụ của rơle bảo vệ
- Nguồn điện được khôi phục thủ công trong vòng vài giờ

Trang trại điện gió tại Đức 2022



- Mã độc tống tiền trên CNTT
- Công ty vận hành và bảo trì trang trại gió
- Mạng CNTT/OT bị ngắt kết nối
- Trang trại gió tiếp tục ở Chế độ Đảo

Triton / Trisis 2017



- PLC an toàn bị xâm phạm và buộc phải thực hiện hành động không an toàn
- hệ thống ngắt rơle bảo vệ an toàn

Các cuộc tấn công vào cơ sở hạ tầng trước đây phần lớn không hiệu quả. Để một cuộc tấn công gây hư hỏng thiết bị, cần có cả hai điều kiện sau:

- phải bắt buộc có một điều kiện hoạt động không an toàn
- hệ thống bảo vệ bị vô hiệu hóa thường là dư thừa

DNV

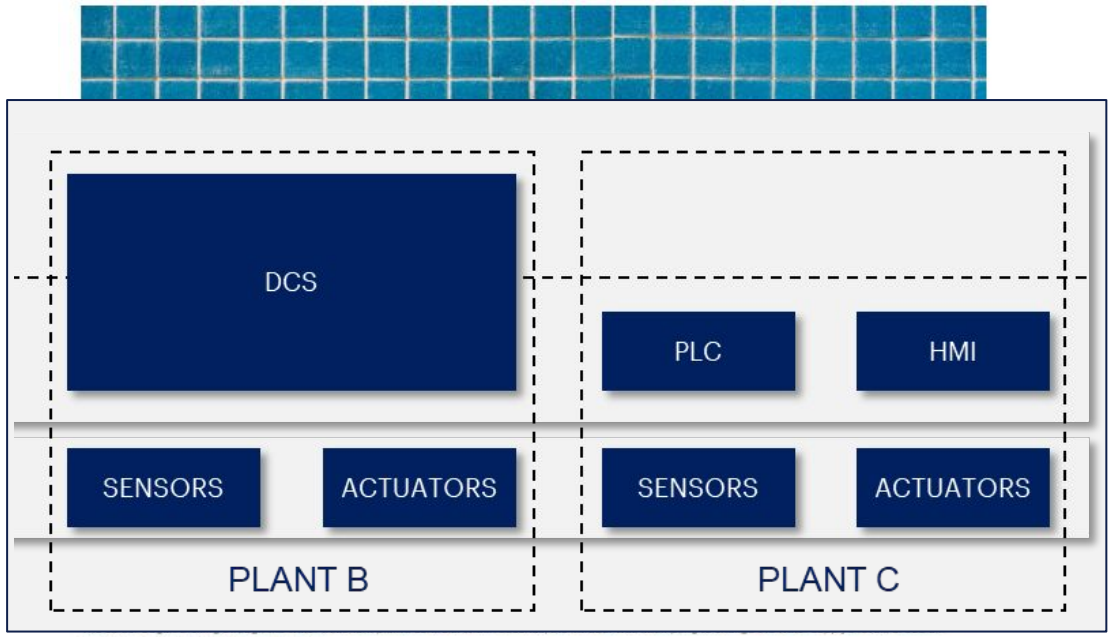
Ví dụ về kỹ thuật thông tin mạng



ANDY GREENBERG SECURITY FEB 8, 2021 6:54 PM

A Hacker Tried to Poison a Florida City's Water Supply, Officials Say

The attacker upped sodium hydroxide levels in the Oldsmar, Florida, water supply to extremely dangerous levels.



hydroxide. PHOTOGRAPH: GETTY IMAGES

Cách triển khai Kỹ thuật thông tin mạng

- Yêu cầu có sự tham gia của và đào tạo cho đội ngũ kỹ thuật và thiết kế
- Cơ hội giảm thiểu hoặc thậm chí loại bỏ khả năng xảy ra một cuộc tấn công vật lý trên mạng
- 12 nguyên tắc thiết kế xuyên suốt 7 giai đoạn thiết kế
- Hướng dẫn thực hiện được phát triển bởi Phòng thí nghiệm quốc gia Idaho



Yêu cầu về quản trị – Nguyên tắc thiết kế an ninh mạng

- CIIO phải áp dụng các nguyên tắc sau đây đối với con người, quy trình và công nghệ:
  - Phòng thủ theo chiều sâu
  - Đặc quyền tối thiểu
  - Phân công nhiệm vụ
- CIIO cũng phải áp dụng (nếu có thể)
  - Phòng thủ bằng sự đa dạng
    - Công nghệ, nhà cung cấp, lộ trình, v.v.
  - Không tin tưởng
    - Mỗi yêu cầu truy cập phải được xác thực, ủy quyền và xác nhận



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Yêu cầu về quản trị – Quản lý thay đổi

- CIIO phải thiết lập quy trình quản lý thay đổi cho tất cả các thay đổi trong CII
  - Nhận diện
  - Ủy quyền
  - Thực hiện
  - Xác nhận



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

DNV ©

Yêu cầu về quản trị – Quản lý thay đổi thành phần cấu hình

- Quy trình bằng văn bản phải được thực hiện
  - Xây dựng cấu hình cơ sở cho hệ điều hành, phần mềm, cổng và bản vá bảo mật
  - Ủy quyền và ghi lại những thay đổi khác với bản cơ sở
  - Cập nhật cấu hình cơ sở, nếu cần, trong vòng 30 ngày dương lịch
  - Xác minh hiệu quả của các biện pháp kiểm soát mạng sau thay đổi
  - Xác minh danh tính nguồn và tính toàn vẹn của phần mềm
  - Theo dõi những thay đổi so với bản cơ bản sau mỗi 35 ngày

- CIP-010-4



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DNV

Yêu cầu về quản trị – Sử dụng hệ thống và dịch vụ điện toán đám mây

- CIIO vẫn chịu trách nhiệm VÀ trách nhiệm giải trình ngay cả khi CII được triển khai trên nền tảng đám mây
- CIIO phải thông báo cho ủy viên về tất cả các kế hoạch triển khai trên nền tảng đám mây
  - Mô hình triển khai (công khai, riêng tư, kết hợp)
  - Mô hình dịch vụ (SaaS, PaaS, IaaS)
- CIIO phải đảm bảo bên cung cấp dịch vụ đám mây chỉ định một đại diện được ủy quyền ở Singapore để tiếp nhận công văn hay thư thông báo



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Yêu cầu về quản trị – Quản lý nhà cung cấp và dịch vụ thuê ngoài

- CIIO vẫn chịu trách nhiệm VÀ có trách nhiệm giải trình ngay cả khi các hoạt động được thuê ngoài
- CIIO phải thiết lập các quy trình để duy trì giám sát tất cả các hoạt động thuê ngoài
- Phải bao gồm các điều khoản trong thỏa thuận dịch vụ thuê ngoài
  - Loại quyền truy cập/tiếp cận CII
  - Nghĩa vụ bảo vệ CII khỏi các mối đe dọa mạng
  - Nghĩa vụ báo cáo sự cố mạng
  - Quyền của CIIO trong việc kiểm toán tình hình an ninh mạng của bên thứ ba
- Phải thiết lập quy trình để xác minh tính tuân thủ



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Yêu cầu về quản trị – Quản lý rủi ro chuỗi cung ứng

- Quy trình bằng văn bản phải được rà soát, phê duyệt và thực hiện
  - Kế hoạch mua sắm Hệ thống mạng của BES và các EACMS và PACS liên quan
  - Thông báo của nhà cung cấp về các sự cố do nhà cung cấp xác định
  - Phối hợp ứng phó
  - Thông báo từ nhà cung cấp khi không còn được cấp quyền truy cập từ xa hoặc tại chỗ
  - Công bố thông tin của các nhà cung cấp về các lỗ hổng đã biết
  - Xác minh tính toàn vẹn và tính xác thực của phần mềm
- CIP-013-2



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DNV

Nghiên cứu trường hợp về chuỗi cung ứng

DNV ©

27 Tháng 11 năm 2013 - Vi phạm mục tiêu thông qua nhà cung cấp HVAC

- Lộ 40 triệu tài khoản thẻ tín dụng và thẻ ghi nợ
- Vi phạm thông qua Nhà cung cấp bên thứ ba phục vụ hệ thống sưởi và làm mát
- Thiết kế mạng phẳng đã cho phép kẻ tấn công đến được các tài sản xung yếu một cách dễ dàng

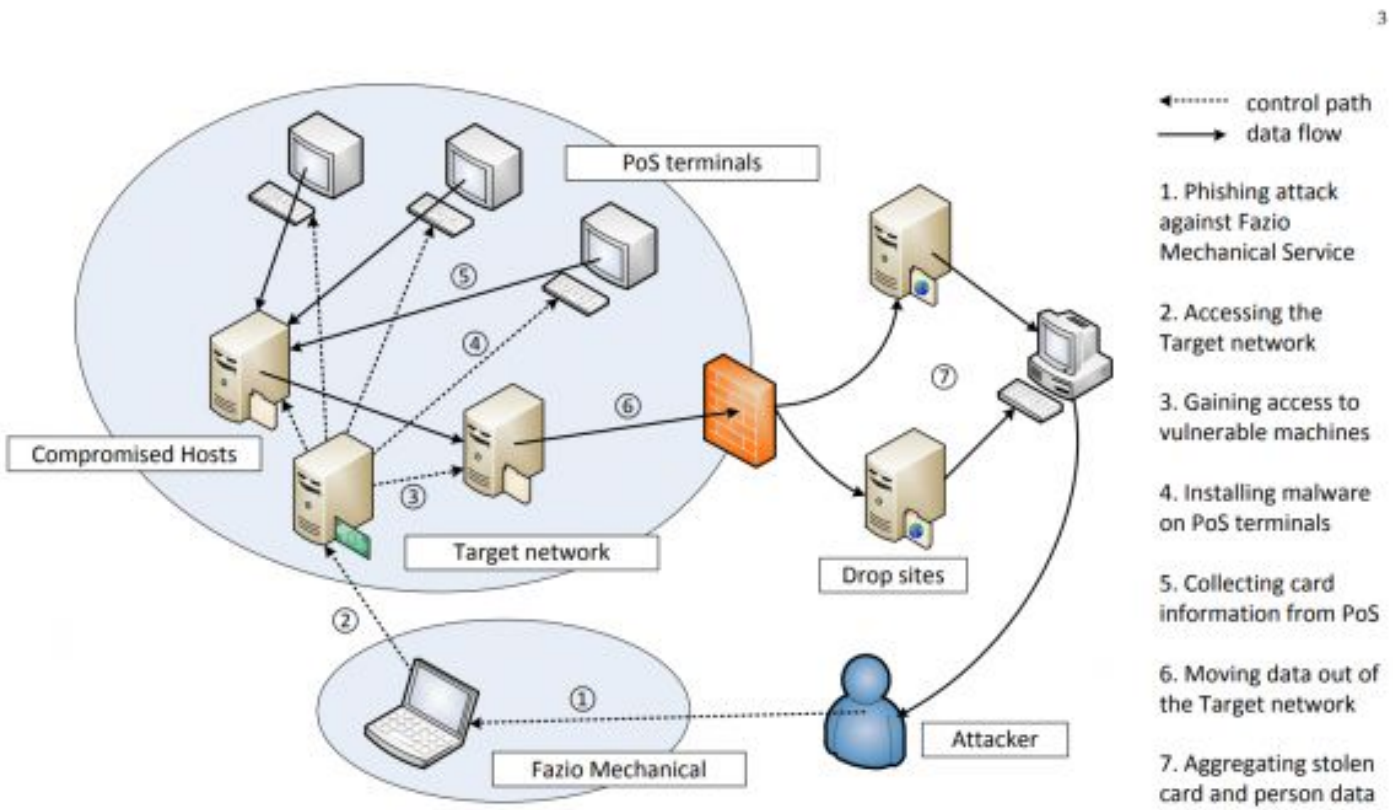


Fig. 2. Attack steps of the Target breach.

Tháng 12 năm 2020 - SolarWinds



Nhà cung cấp hàng đầu về hệ thống CNTT, nền tảng giám sát và quản lý mạng

Hàng triệu mạng trên toàn cầu bao gồm các mạng của chính phủ, Apple, Amazon, Google, v.v.

Truy cập được tin cậy xâm nhập sâu vào các mạng được triển khai

- Tin tặc cấp cao, tầm quốc gia
- Các công cụ của nhà cung cấp bị xâm phạm
- Được thiết kế có thể dành cho hoạt động gián điệp của chính phủ Hoa Kỳ và các tổ chức thân cận
- Là một phần trong cuộc tấn công chuỗi cung ứng trên toàn thế giới
- Thúc đẩy sự gia tăng nhanh chóng áp lực pháp lý đối với an ninh chuỗi cung ứng
- 39,8 triệu USD được bảo hiểm bù đắp một phần

DNV ©

DNV

An ninh chuỗi cung ứng

DNV ©

Các phương pháp thực hành chính trong quản lý rủi ro chuỗi cung ứng mạng

- Tạo các vai trò, cấu trúc và quy trình hợp tác rõ ràng cho chuỗi cung ứng, an ni mạng, an ninh sản phẩm, an ninh vật lý và các chức năng liên quan khác.
- Tích hợp các cân nhắc về an ninh mạng vào hệ thống và vòng đời sản phẩm.
- Xác định mức độ quan trọng của nhà cung cấp bằng cách sử dụng các tiêu chuẩn ngành và các thực hành tốt nhất .
- Cố vấn và huấn luyện các nhà cung cấp để cải thiện hoạt động an ninh mạng của họ.
- Bao gồm các nhà cung cấp chính trong việc lập kế hoạch dự phòng sự cố (CP), ứng phó sự cố (IR), lập kế hoạch phục hồi sau thảm họa và kiểm thử.
- Sử dụng đánh giá của bên thứ ba, thăm thực địa và cấp chứng nhận chính thức để đánh giá các nhà cung cấp quan trọng.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8276

DNV

ENTSO-E Quy chuẩn mạng lưới về an ninh mạng

Mạng lưới các đơn vị vận hành hệ thống truyền tải điện của Châu Âu

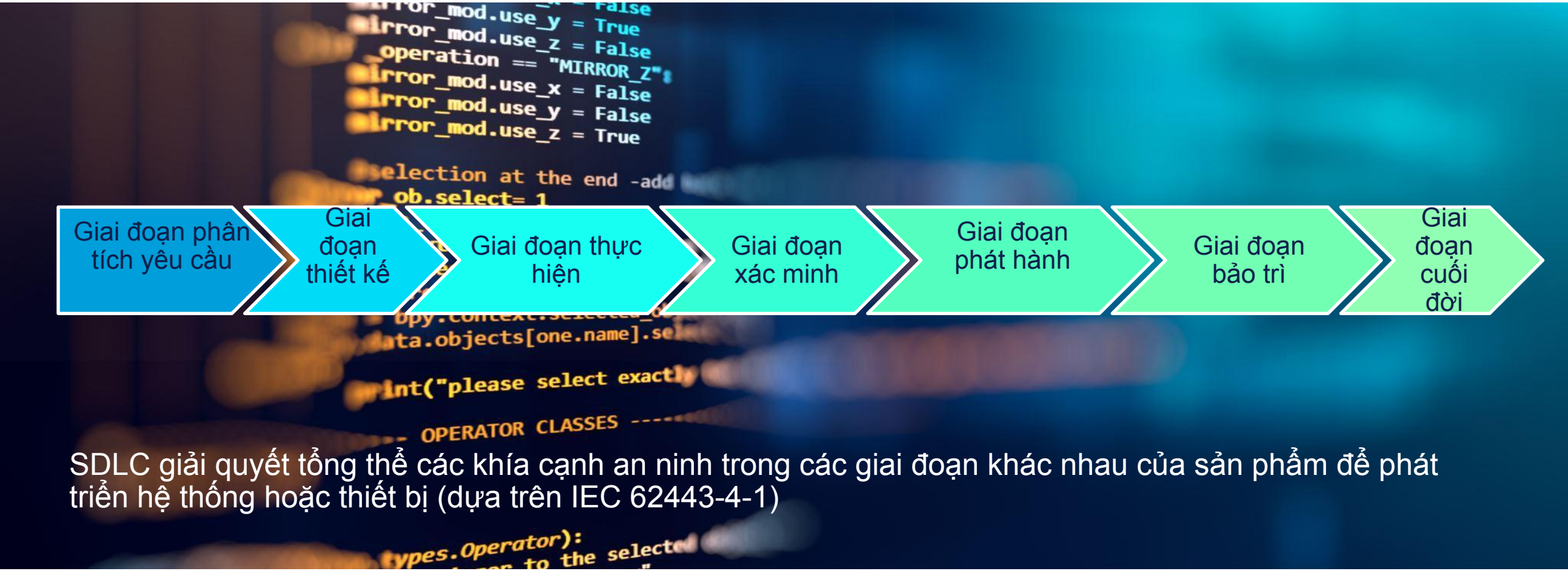
Hướng dẫn về chuỗi cung ứng mạng có liên quan (Điều 27)

- Đưa các yêu cầu về an ninh mạng vào các yêu cầu mua sắm đối với các sản phẩm, dịch vụ và quy trình CNTT bao gồm ít nhất:
  - yêu cầu mua sắm kỹ thuật an ninh mạng đối với sản phẩm CNTT, dịch vụ CNTT hoặc quy trình CNTT được sử dụng hoặc sẽ được sử dụng
  - kiểm tra xác minh lý lịch của nhân viên của nhà cung cấp tham gia vào chuỗi cung ứng và xử lý thông tin nhạy cảm hoặc quyền truy cập vào tài sản có tác động cao
  - các quy trình để thiết kế, phát triển và sản xuất các sản phẩm, dịch vụ và quy trình CNTT một cách an toàn và có kiểm soát, thúc đẩy kiến trúc an ninh mạng theo thiết kế và nguyên tắc ***Không tin cậy***
  - kiểm soát quyền truy cập của nhà cung cấp vào tài sản của đơn vị
  - tuyên truyền về các yêu cầu mua sắm an ninh mạng cho các nhà thầu phụ của nhà cung cấp
  - truy vết theo dõi việc áp dụng các yêu cầu mua sắm an ninh mạng từ quá trình phát triển đến sản xuất cho đến khi giao hàng
  - hỗ trợ cập nhật an ninh trong suốt vòng đời của sản phẩm CNTT, dịch vụ CNTT hoặc quy trình CNTT; Và
  - duy trì quyền kiểm tra các quy trình thiết kế, phát triển và sản xuất của nhà cung cấp.
- Chỉ lựa chọn và ký hợp đồng với các nhà cung cấp có thể đáp ứng các yêu cầu mua sắm an ninh mạng và có mức độ an ninh mạng phù hợp với rủi ro an ninh mạng của sản phẩm, dịch vụ hoặc quy trình CNTT
- Đa dạng hóa nguồn cung cấp các sản phẩm, dịch vụ và quy trình CNTT và hạn chế việc bắt buộc phải gắn chặt với nhà cung cấp;
- Giám sát, đánh giá hoặc kiểm tra các yêu cầu mua sắm an ninh mạng cho các quy trình của nhà cung cấp trong toàn bộ vòng đời

Vòng đời phát triển an toàn

DNV ©

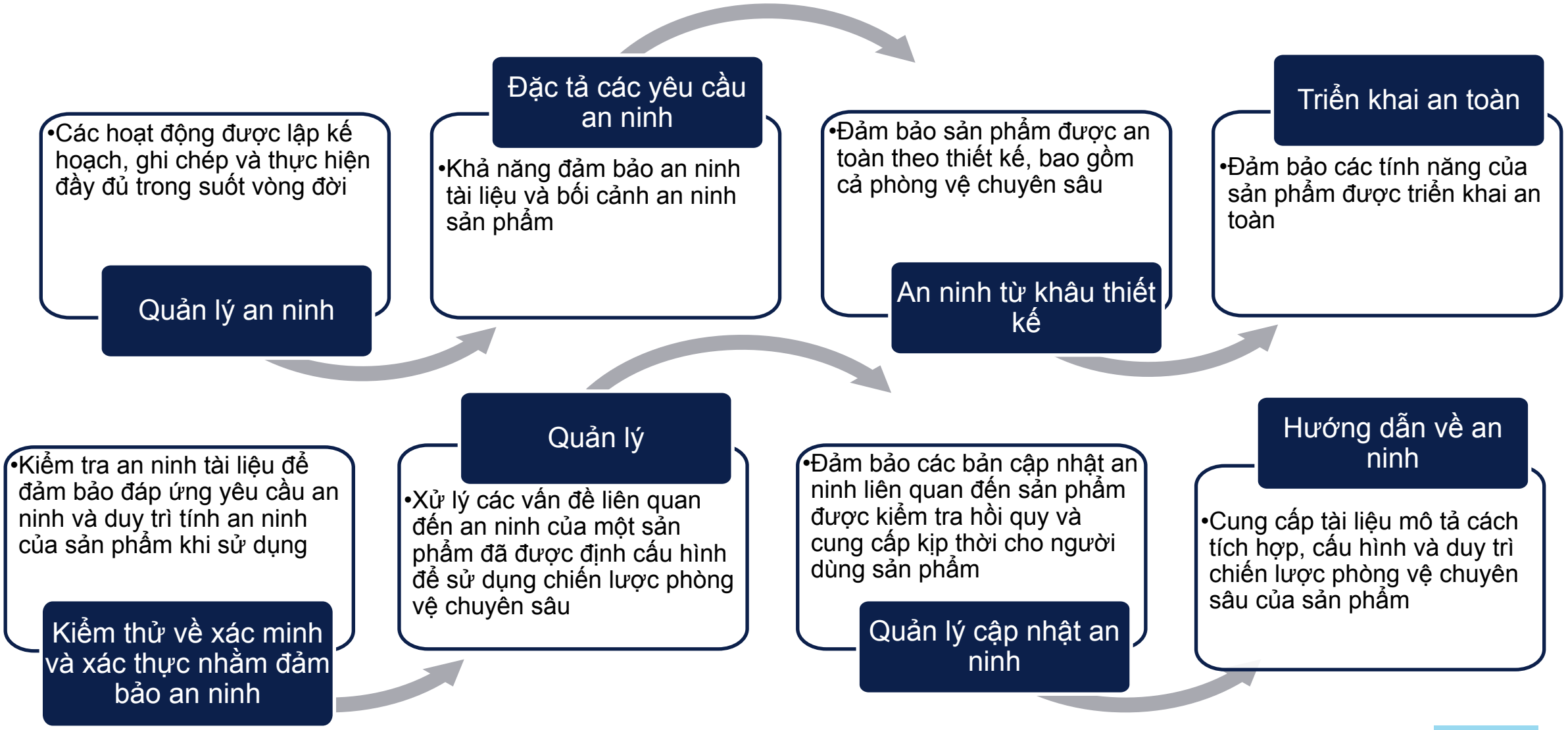
Vòng đời phát triển an toàn (SDLC)



SDLC giải quyết tổng thể các khía cạnh an ninh trong các giai đoạn khác nhau của sản phẩm để phát triển hệ thống hoặc thiết bị (dựa trên IEC 62443-4-1)

DNV ©

Thực hành SDLC theo tiêu chuẩn IEC 62443-4-1



DNV ©

Các nguồn tư liệu bổ sung

DNV ©

Chứng nhận sản phẩm của bên thứ ba

Đạo luật về khả năng chống chịu trên môi trường mạng (EU)

Các yêu cầu ghi nhãn của Hoa Kỳ, chứng nhận an ninh mạng UL

Chứng nhận quy trình SDLC IEC 62443-4-1 (dành cho nhà cung cấp sản phẩm)

Chứng nhận thành phần IEC 62443-4-2 (dành cho nhà cung cấp sản phẩm)

Chứng nhận hệ thống IEC 62443-3-3 (dành cho nhà cung cấp sản phẩm)

Chứng nhận đánh giá tại thực địa IEC 62443-2-1, -2-4, -3-2, -3-3 (dành cho chủ sở hữu hệ thống)

Bằng chứng của nhà cung cấp về kiểm thử của bên thứ ba

DNV ©

Tài liệu tham khảo thông tin

Yêu cầu mua sắm

Ngôn ngữ mua sắm an ninh mang cho hê thống điều khiển (cisa.gov)

Điều khoản ngôn ngữ mua sắm an ninh mang cho hợp đồng RFP và EVSP · Văn phòng chung về năng lương và vân tải (driveelectric.gov)

Bảng câu hỏi an ninh

VSAQ - Bảng câu hỏi đánh giá an ninh (vsaq-demo.withgoogle.com)

Các tư liệu khác

Chứng nhận (isasecure.org)

Tiêu chuẩn | IECEE

DNV ©

Tóm tắt

- Yêu cầu:
  - Ưu tiên các phát hiện từ hoạt động kiểm toán và kế hoạch khắc phục
  - Vai trò, trách nhiệm rõ ràng và phân công cho nhân sự quen với các vấn đề an ninh mạng
  - Đánh giá rủi ro
  - Chính sách
  - Quản lý thay đổi
  - Quản lý chuỗi cung ứng
- CCoP của Singapore
- Phương pháp đánh giá rủi ro
- Lồng ghép an ninh mạng từ thiết kế

Yêu cầu về Nhận diện và Bảo vệ

DNV ©

Yêu cầu về nhận diện – Quản lý tài sản

- CIIO phải thiết lập các cơ chế và quy trình để xác định tất cả tài sản CII và cập nhật danh mục tài sản
- Phải cập nhật danh mục bất cứ khi nào có thay đổi



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

DNV ©

Kiểm kê tài sản – cần bao nhiêu thông tin chi tiết?

- Chủ sở hữu và đơn vị vận hành
- Tên
- Mô tả chức năng trọng yếu
- Người phụ trách chính về an ninh mạng
- Sự phụ thuộc và kết nối giữa tài sản và bất kỳ hệ thống nội bộ / bên ngoài nào
- Vị trí vật lý
- Đơn vị cung cấp dịch vụ thuê ngoài
- Dịch vụ đám mây được sử dụng (nếu có)
- Liên kết Internet hỗ trợ CII
- Sơ đồ cấu trúc mạng
- Nhà sản xuất và mẫu
- Cổng giao tiếp (Ethernet, nối tiếp, v.v.)
- Địa chỉ IP, địa chỉ MAC
- Phần mềm chính, phiên bản
- Dịch vụ đang chạy

DNV ©

Yêu cầu về bảo vệ – Kiểm soát truy cập

- CIIO phải đảm bảo rằng quyền truy cập/tiếp cận CII và giữa các bộ phận của CII chỉ dành cho nhân sự và thiết bị được duyệt
- Nhà cung cấp truy cập/tiếp cận CII phải
  - Được ghi lại bằng văn bản
  - Có chấp thuận từ trước
  - Được giám sát bởi CIIO
  - Làm việc tại chỗ
- Phải tự động chấm dứt phiên đăng nhập sau khi không hoạt động trong khoảng thời gian định trước
- Nếu không thể tự động chấm dứt phiên đăng nhập, CIIO phải theo dõi hoạt động bất thường



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

DNV ©

Yêu cầu về bảo vệ – Kiểm soát truy cập

- Chương trình quản lý tiếp cận vật lý và truy cập điện tử bằng văn bản phục vụ xử lý và giảm thiểu sự cố của BES phải được triển khai
  - Quy trình ủy quyền
  - Xác minh mỗi quý
- Chương trình thu hồi quyền truy cập bằng văn bản phải được thực hiện
- Chương trình quản lý truy cập BCSI bằng văn bản phục vụ xử lý và giảm thiểu sự cố của BES phải được triển khai

- CIP-004-7



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DNV

Yêu cầu về bảo vệ – An ninh vật lý

- Kế hoạch an ninh vật lý bằng văn bản phục vụ xử lý và giảm thiểu sự cố của BES phải được triển khai
  - Biện pháp kiểm soát hoạt động hoặc thủ tục để hạn chế quyền tiếp cận vật lý
  - Kiểm soát tiếp cận vật lý để hạn chế quyền tiếp cận vật lý không có người giám sát chỉ dành cho những cá nhân được ủy quyền
  - Giám sát việc tiếp cận trái phép và đưa ra cảnh báo trong vòng 15 phút
  - Ghi nhật ký và lưu giữ trong 90 ngày
  - Hạn chế tiếp cận vật lý vào hệ thống cáp
  - Việc tiếp cận liên tục có người giám sát của khách tham quan
  - Bảo trì và kiểm thử hệ thống kiểm soát 24 tháng/lần

- CIP-006-6



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DNV ©

Yêu cầu về bảo vệ – An ninh vật lý

- Thực hiện đánh giá rủi ro ban đầu và các đánh giá rủi ro tiếp theo đối với các trạm truyền tải và trạm biến áp truyền tải
- Bên thứ ba không liên kết sẽ xác minh đánh giá rủi ro
- Tiến hành đánh giá các mối đe dọa và lỗ hổng tiềm ẩn liên quan đến cuộc tấn công vật lý
- Xây dựng và thực hiện kế hoạch an ninh vật lý bằng văn bản
- Bên thứ ba không liên kết rà soát kết quả đánh giá và kế hoạch an ninh vật lý

- CIP-014-3



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DNV

Yêu cầu về bảo vệ – Quản lý tài khoản

- CIIO phải cấp quyền tối thiểu cho mỗi tài khoản để thực hiện các chức năng
- Quyền cài đặt phần mềm chỉ được cấp cho các tài khoản được duyệt
- Không dùng chung tài khoản, trừ khi cần thiết cho hoạt động CII
- Theo dõi hoạt động của từng tài khoản
- Xóa hoặc vô hiệu hóa các tài khoản không hoạt động và không cần thiết
- Phải rà soát tất cả các tài khoản gửi đến CII ít nhất 12 tháng/lần



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Yêu cầu về bảo vệ – Quản lý quyền truy cập đặc biệt

- CIIO chỉ được cấp quyền truy cập đặc biệt cho các tài khoản được chọn
- Phải duy trì danh mục cập nhật các tài khoản được cấp quyền đặc biệt (bao gồm thông tin chi tiết về quyền và đặc quyền)
- Phải sử dụng MFA (xác thực đa yếu tố)
- Quyền truy cập đặc biệt phải đến từ môi trường mạng được củng cố
- Việc truyền dữ liệu phải thông qua các kết nối được phê duyệt



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Yêu cầu về bảo vệ – Bộ điều khiển miền

- CIIO phải triển khai cơ chế giám sát những thay đổi trong mối quan hệ tin cậy giữa các miền



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Yêu cầu về bảo vệ – Phân đoạn mạng

- CIIO phải phân đoạn kiến trúc mạng CII dựa trên mức độ bảo mật và rủi ro
- Việc giao tiếp giữa các phân đoạn CII khác nhau phải được giới hạn ở mức tối thiểu cần thiết cho hoạt động CII
- Phải triển khai cơ chế bảo mật mạng để phát hiện và chặn lưu lượng mạng độc hại
- Phải thiết lập cơ chế cô lập phân đoạn CII bị ảnh hưởng bởi sự cố mạng



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Yêu cầu về bảo vệ – Vành đai an ninh mạng điện tử (ESP)

- Quy trình bằng văn bản phải được thực hiện
  - ESP xác định cho các tài sản được kết nối với mạng thông qua giao thức định tuyến (= vùng)
  - Có thể định tuyến bên ngoài thông qua Điểm truy cập điện tử xác định (= ống dẫn)
  - quyền truy cập vào và ra, và mặc định từ chối (= quy tắc tường lửa)

- CIP-005-7



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DNV

Yêu cầu về bảo vệ – Bảo mật mạng

- Các quy tắc kiểm soát truy cập mạng cho CII phải được triển khai và rà soát định kỳ
- CII không được kết nối với mạng bên ngoài hoặc internet, trừ khi cần thiết cho hoạt động
- Nếu CII yêu cầu kết nối bên ngoài:
  - cơ chế bảo mật mạng để phát hiện và chặn lưu lượng mạng độc hại và giao tiếp mạng an toàn phải được triển khai
  - Hướng luồng dữ liệu hạn chế theo một chiều nếu có thể



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Yêu cầu về bảo vệ – Kết nối từ xa

- Phải triển khai các biện pháp kiểm soát mạng hiệu quả cho tất cả các kết nối từ xa tới CII
  - Ngăn chặn và phát hiện truy cập trái phép
  - Xác thực kết nối từ xa được duyệt
- Kết nối từ xa tới CII phải bị vô hiệu hóa, trừ khi cần thiết cho hoạt động
- Phải sử dụng MFA
- Phải sử dụng mã hóa mạnh
- Tệp tải lên CII phải được quét phần mềm độc hại
- Luồng dữ liệu phải được giới hạn ở mức tối thiểu cần thiết



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Yêu cầu về bảo vệ – Truy cập từ xa

- Quy trình bằng văn bản phải được thực hiện
  - Hệ thống trung gian (= máy chủ trung gian)
  - Mã hóa kết thúc tại Hệ thống trung gian (= vpn)
  - MFA
  - Phương pháp giám sát và vô hiệu hóa các phiên làm việc từ xa đang hoạt động
  - Phương pháp giám sát và vô hiệu hóa kết nối từ xa do nhà cung cấp đã xác thực khởi tạo

- CIP-005-7



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DNV

Yêu cầu về bảo vệ – Kết nối không dây

- CII không được kết nối với WLAN trừ khi cần thiết cho hoạt động vận hành
- Nếu CII yêu cầu kết nối WLAN:
  - Chỉ được sử dụng WLAN được duyệt
  - Phải sử dụng mã hóa mạnh
  - Chỉ các thiết bị CII được duyệt mới được phép kết nối với WLAN



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Yêu cầu về bảo vệ – Tăng cường hệ thống

- Cấu hình cơ sở bảo mật phải được triển khai cho các loại tài sản CII được liệt kê
- Cấu hình cơ sở bảo mật phải được rà soát ít nhất 12 tháng/lần
- Chỉ những thiết bị được duyệt chuyên dụng mới được sử dụng để quản lý CII



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Các loại tài sản CII phải có cấu hình cơ sở

- Hệ điều hành (OS)
- Thiết bị gia dụng
- Bàn điều khiển và máy trạm
- Thiết bị mạng
- Máy chủ
- Ứng dụng phần mềm

Thực hành bảo mật tối thiểu

- Quản lý tài khoản
- Quản lý mật khẩu và cụm mật khẩu
- Kiểm soát ứng dụng
- Cổng và dịch vụ
- Kết nối vật lý
- Bảo vệ khỏi phần mềm độc hại
- Cập nhật và nâng cấp phần mềm

Yêu cầu về bảo vệ – Quản lý bảo mật hệ thống

- Quy trình bằng văn bản phải được thực hiện
  - Chỉ bật các cổng cần thiết
  - Bảo vệ khỏi việc sử dụng các cổng đầu vào/đầu ra vật lý không cần thiết

- CIP-007-6



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DNV

Yêu cầu về bảo vệ – Quản lý bản vá

- CIIO phải triển khai quy trình quản lý bản vá bảo mật
- Phải đảm bảo cấp quản lý giám sát hiệu quả của quy trình.



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Quy trình quản lý bản vá bảo mật phải bao gồm

- Theo dõi việc phát hành bản vá bảo mật cho các tài sản CII
- Xác minh tính toàn vẹn của bản vá bảo mật
- Kiểm tra các bản vá bảo mật trong môi trường kiểm thử (QAS) tương tự như môi trường sản xuất
- Lập ưu tiên áp dụng các bản vá bảo mật
- Áp dụng bản vá bảo mật
- Theo dõi và giám sát tiến trình vá lỗi
- Áp dụng kiểm soát bù trừ nếu không thể vá lỗi
- Hủy bỏ việc áp dụng các bản vá bảo mật

Yêu cầu về bảo vệ – Quản lý bảo mật hệ thống

- Quy trình bằng văn bản phải được thực hiện
  - Quy trình quản lý bản vá để theo dõi, đánh giá và cài đặt các bản vá bảo mật
  - Đánh giá các bản vá bảo mật để đảm bảo khả năng áp dụng theo định kỳ ít nhất 35 ngày/lần
  - Kế hoạch ứng dụng bản vá hoặc kế hoạch giảm thiểu

- CIP-007-6



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DNV

Yêu cầu về bảo vệ – Thiết bị máy tính di động và phương tiện lưu trữ di động

- CIIO phải thiết lập quy trình để ủy quyền và theo dõi việc sử dụng các thiết bị máy tính di động và phương tiện lưu trữ di động trong CII
- Các thiết bị di động được duyệt phải tuân thủ theo cấu hình bảo mật cơ sở
- Các thiết bị di động được duyệt phải không chứa phần mềm độc hại trước khi kết nối với CII
- Sử dụng mã hóa mạnh cho dữ liệu nhạy cảm của CII lưu trữ trong thiết bị được duyệt



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

DNV ©

Yêu cầu về bảo vệ – Bảo mật ứng dụng

- Chỉ những ứng dụng được CIIO chấp thuận mới được sử dụng trong CII
- Danh sách đề nghị đã được chấp thuận phải được rà soát ít nhất 12 tháng/lần
- Xác minh tính toàn vẹn của ứng dụng trước khi sử dụng trong CII
- Kiến trúc đa tầng cho hệ thống CNTT của CII
- Ứng dụng web phải tuân theo các hướng dẫn mới nhất của OWASP
- Ứng dụng web kết nối Internet phải có tường lửa ứng dụng web (WAF)
- Trình biên dịch và trình gỡ lỗi phải được gỡ bỏ khi không còn cần thiết



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Yêu cầu về bảo vệ – Bảo mật cơ sở dữ liệu

- Chỉ những tài khoản được ủy quyền mới có thể kết nối và truy vấn cơ sở dữ liệu trong CII
- Quản trị hệ thống và quản trị cơ sở dữ liệu phải được tách biệt và giao cho những người khác nhau
- Các chính sách bảo mật cơ sở dữ liệu CII phải được thiết lập
  - Cách bảo mật dữ liệu khi lưu trữ
  - Làm thế nào để ngăn chặn rò rỉ dữ liệu
  - Làm thế nào để hạn chế quyền truy cập dữ liệu nhạy cảm chỉ dành cho những người được ủy quyền
- Giám sát cơ sở dữ liệu CII để tìm các hoạt động bất thường (bao gồm các truy vấn hàng loạt vượt quá ngưỡng)



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

DNV

Yêu cầu về bảo vệ – Bảo vệ thông tin

- Quy trình bằng văn bản phải được thực hiện
  - Các phương pháp bảo vệ và xử lý thông tin hệ thống mạng của BES (BCSI) một cách an toàn để giảm thiểu rủi ro xâm phạm tính bảo mật
  - Ngăn chặn việc truy xuất trái phép BCSI từ phương tiện lưu trữ dữ liệu của Tài sản mạng trước khi phát hành để tái sử dụng
  - Ngăn chặn việc truy xuất BCSI trái phép từ Tài sản mạng hoặc phá hủy phương tiện lưu trữ dữ liệu trước khi xử lý

- CIP-011-3



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DNV

Yêu cầu về bảo vệ – Đánh giá lỗ hổng (VA)

- Phải có quy trình để xác định và theo dõi các lỗ hổng bảo mật mạng trong CII
- Tất cả các lỗ hổng bảo mật mạng phải được khắc phục kịp thời
- VA của CII phải được thực hiện
  - Định kỳ 12 tháng/lần (đối với CNTT)
  - Định kỳ 24 tháng/lần (đối với OT)
- VA phải được thực hiện sau những thay đổi lớn của hệ thống
- Báo cáo VA và kế hoạch khắc phục phải được trình Ủy viên trong vòng 30 ngày làm việc theo yêu cầu



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Yêu cầu về bảo vệ – Đánh giá lỗ hổng (VA)

- Quy trình bằng văn bản phải được thực hiện
  - Tiến hành VA dựa trên tài liệu hoặc chủ động 15 tháng/lần
  - Tiến hành VA chủ động phục vụ xử lý sự cố của BES 36 tháng/lần
  - Tiến hành VA chủ động phục vụ xử lý sự cố của BES trước khi bổ sung tài sản mới vào môi trường sản xuất

- CIP-010-4



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DNV

Yêu cầu về bảo vệ – Kiểm thử xâm nhập (PT)

- Kiểm thử xâm nhập đối với CII phải được thực hiện
  - Định kỳ 12 tháng/lần (đối với CNTT)
  - Định kỳ 24 tháng/lần (đối với OT)
- PT phải được thực hiện sau những thay đổi lớn của hệ thống
- Đơn vị nhà cung cấp dịch vụ và đơn vị kiểm thử bên thứ ba phải có chứng nhận và chứng chỉ
  - CREST hoặc tương đương
- PT phải được thực hiện dưới sự giám sát của CIIO, đảm bảo không làm gián đoạn hoạt động của CII
- Báo cáo PT và kế hoạch khắc phục phải được trình Ủy viên trong vòng 30 ngày làm việc theo yêu cầu



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

DNV ©

Yêu cầu về bảo vệ – Mô phỏng tấn công đối kháng

- Kế hoạch mô phỏng tấn công nhóm Đỏ/Tím phải được xây dựng
- Mô phỏng tấn công theo nhóm Đỏ/Tím phải được thực hiện ít nhất 24 tháng/lần
- Báo cáo mô phỏng tấn công nhóm Đỏ/Tím và kế hoạch khắc phục phải được trình Ủy viên trong vòng 30 ngày làm việc theo yêu cầu



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Nhóm Đỏ

- Mô phỏng chỉ hoạt động tấn công
- Thời gian đánh giá của nhóm đỏ không được thông báo cho nhóm xanh
- Tập trung vào kiểm thử các biện pháp kiểm soát bảo mật

Nhóm Tím

- Mô phỏng tấn công và phòng thủ
- Thời gian đánh giá của nhóm đỏ được thông báo cho nhóm xanh
- Tập trung kiểm thử các biện pháp kiểm soát an ninh và khả năng ứng phó của nhóm xanh

Những nội dung cần đưa vào Kế hoạch mô phỏng tấn công nhóm Đỏ/Tím

- Mục tiêu
- Các bên liên quan chính
  - nhóm đỏ
  - nhóm xanh
  - đội ngũ quản lý
- Phương pháp đánh giá
  - lập kế hoạch và chuẩn bị tấn công
  - thực hiện tấn công, dọn dẹp và ngăn chặn phát tán
  - báo cáo và đối chiếu của nhóm xanh
  - khuyến nghị và biện pháp khắc phục
- Quy tắc tham gia (chỉ dành cho nhóm đỏ)
- Các biện pháp giảm thiểu để giảm thiểu tác động hoặc ảnh hưởng gián đoạn tiềm ẩn
- Kế hoạch phục hồi

DNV ©

Yêu cầu về bảo vệ – Quản lý khóa mật mã

- Tất cả các khóa mật mã cho CII phải được bảo vệ phòng chống truy cập trái phép
- Các quy trình theo dõi và quản lý vòng đời của khóa mật mã phải được triển khai và rà soát ít nhất 12 tháng/lần



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Tóm tắt

- Nghĩa vụ:
  - Quản lý tài sản
  - Kiểm soát truy cập (vật lý và điện tử)
  - Quản lý tài khoản
  - Phân đoạn mạng
  - Quản lý bản vá
  - Đánh giá lỗ hổng

- CCoP của Singapore
  - Quản lý tài khoản có đặc quyền truy cập
  - Tăng cường hệ thống
  - Kiểm thử xâm nhập
  - Mô phỏng tấn công đối kháng
  - Quản lý khóa mật mã

Yêu cầu quy định về an ninh mạng – Phần 1

Quản lý an ninh mạng trong ngành điện

ivan.christian@dnv.com

+65 9728 2143

www.dnv.com

 DNV ©