CỤC AN TOÀN THÔNG TIN

Giải pháp triển khai đảm bảo an toàn thông tin cho doanh nghiệp

Bình Phước, 08/10/2024

Chuyển đổi số là gì?

Ứng dụng CNTT	Chuyển đổi số
Áp dụng CNTT trên quy trình đã có, trên mô hình hoạt động đã có để cung cấp dịch vụ đã có	Thay đổi quy trình mới Thay đổi mô hình hoạt động mới để cung cấp dịch vụ mới hoặc cung cấp dịch vụ đã có theo cách mới

Ví dụ:
Quản lý sản xuất sản phẩm

Truyền thống

- Quản lý sản xuất sản phẩm bằng lệnh sản xuất (giấy, miệng); theo dõi bán thành phẩm, thành phẩm bằng tay

Ứng dụng CNTT

- Lệnh sản xuất được bộ phận kế hoạch SX chạy từ phần mềm, cấp cho các bộ phận như kho, vật tư; kết quả sản xuất được cập nhật vào phần mềm để theo dõi, tính toán

Chuyển đổi số

- PO (Purchase Order) của khách hàng sẽ lên lịch tự động cho các bộ phận liên quan cung ứng vật tư; sản xuất bằng rô-bốt 24x7; thành phẩm được kiểm tra chất lượng tự động trước khi giao, các thông số và thông tin được ghi nhận tự động.

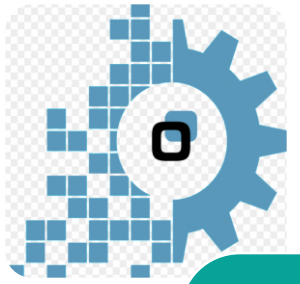
3 cấp độ tiến hoá chuyển đổi số:

Số hoá

- Chuyển dữ liệu analog sang digital

Tin học hoá

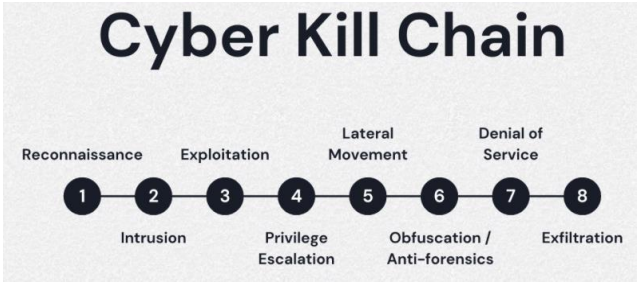
- Tối ưu hóa để tăng hiệu năng hoạt động
- Chưa thực sự thay đổi mô hình, phương thức kinh doanh mới

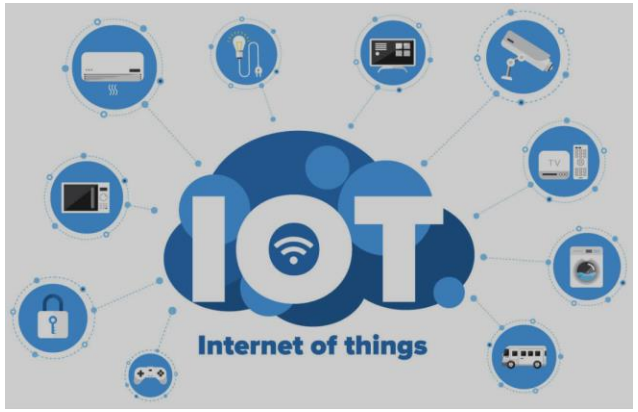


Chuyển đổi số

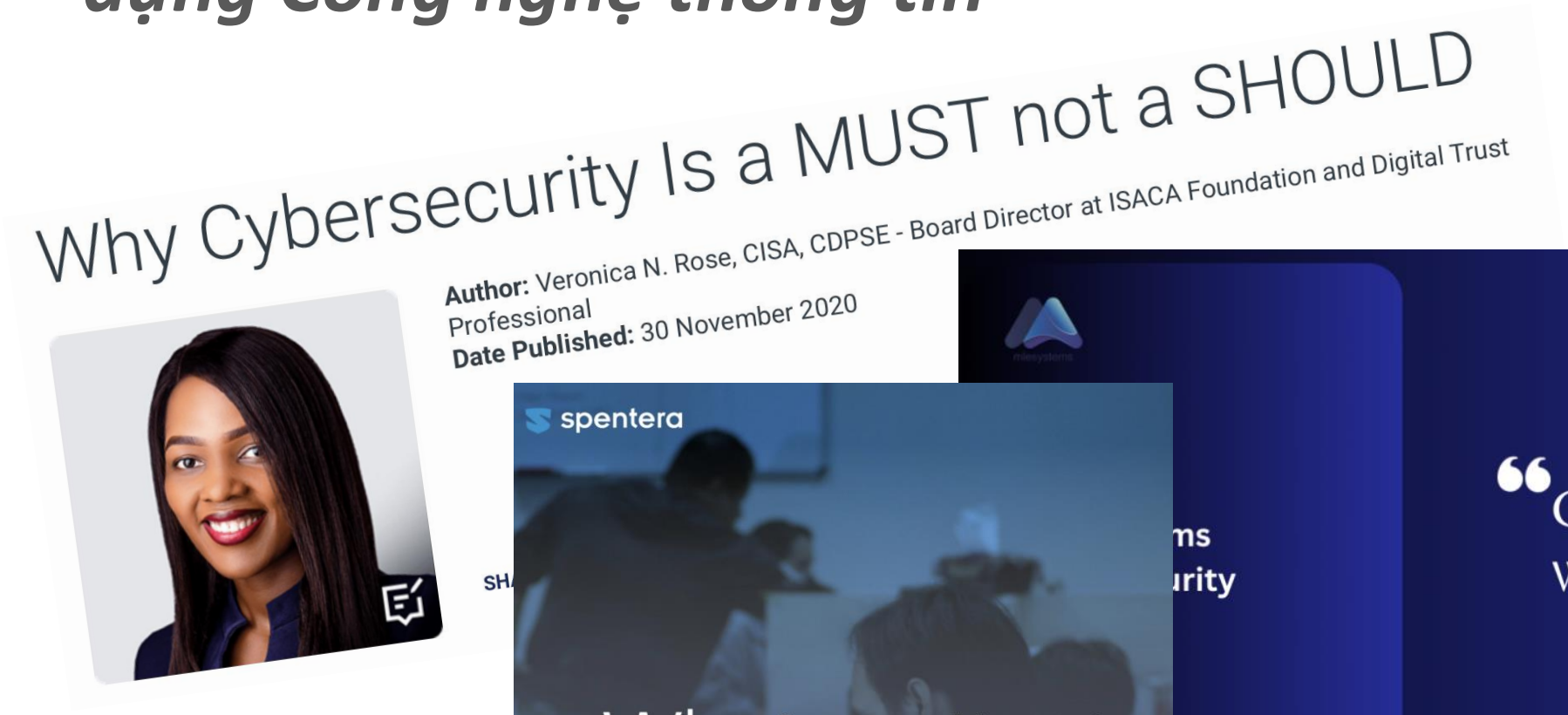
- Quy trình, cách thức hoạt động mới; sản phẩm, dịch vụ mới; mô hình, phương thức kinh doanh mới
- Tận dụng công nghệ, dữ liệu và thông minh hoá

ĐẢM BẢO AN TOÀN LÀ LÀM NHỮNG GÌ ??

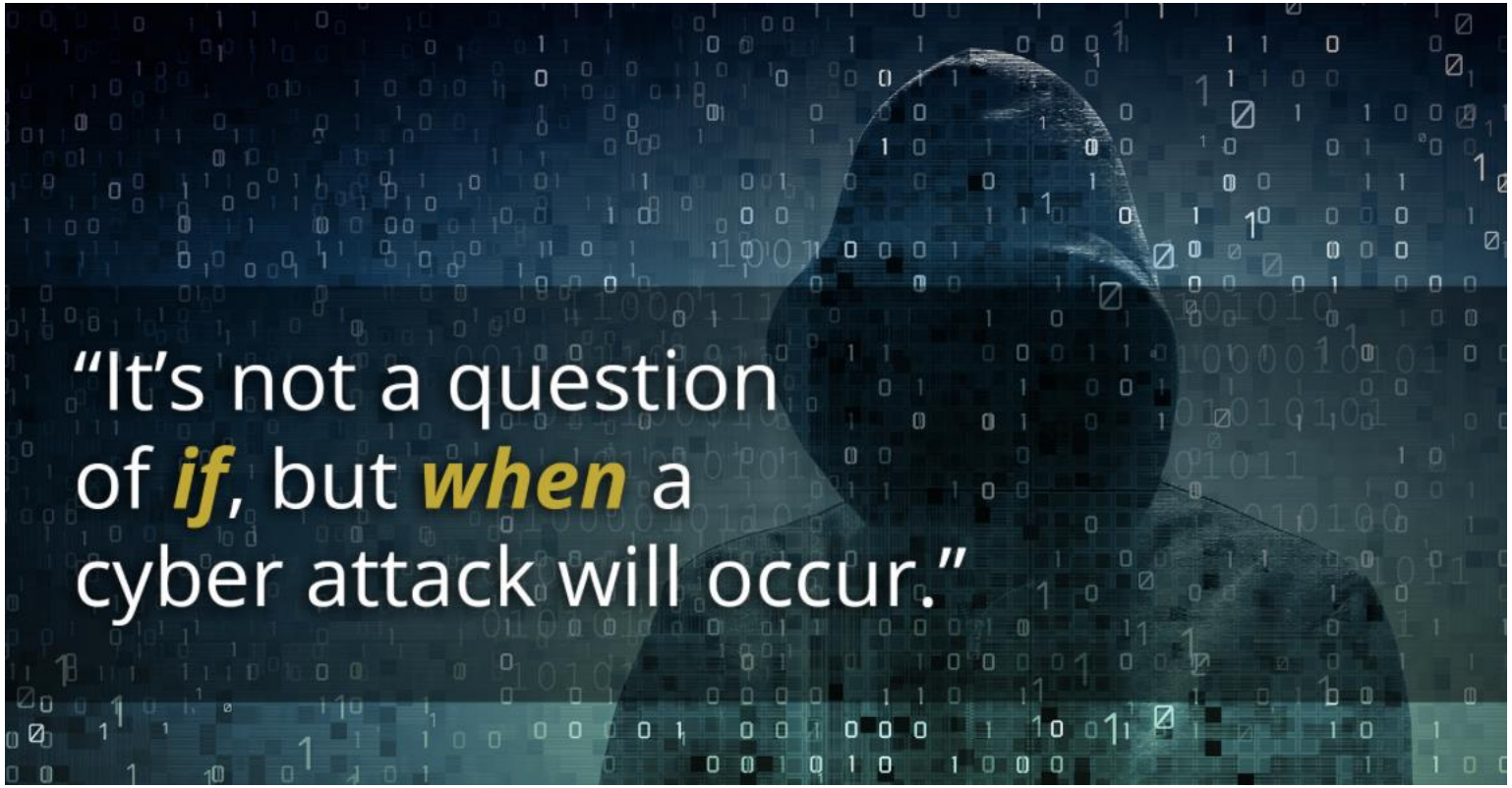




*An toàn thông tin mạng là **PHẢI CÓ** khi triển khai ứng dụng Công nghệ thông tin*



Không còn là "NẾU" bị tấn công mạng, mà là "KHI NÀO" bị tấn công

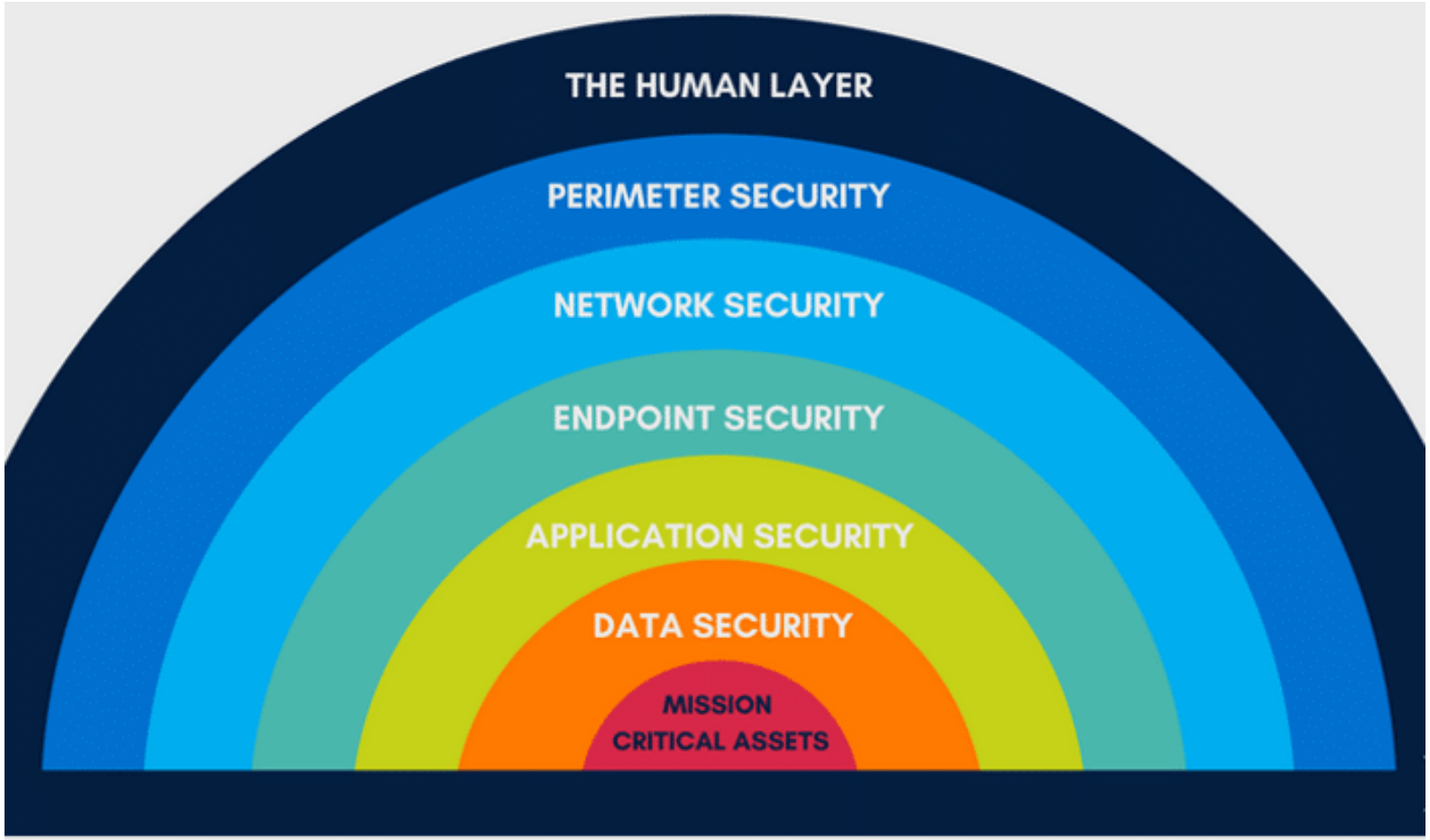


Hãy chuẩn bị cho điều tồi tệ!

TRIỂN KHAI ĐẢM BẢO AN TOÀN THÔNG TIN

CÂU HỎI CỦA NGƯỜI ĐỨNG ĐẦU DOANH NGHIỆP ?

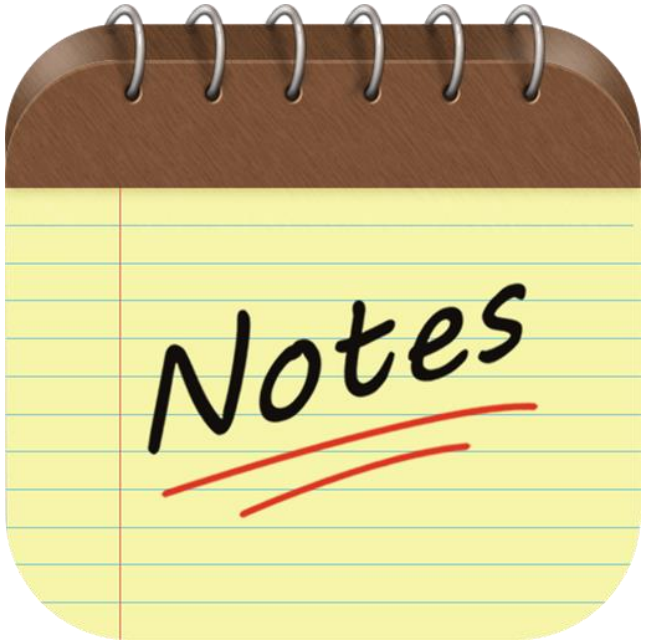
- Doanh nghiệp của tôi có cần phải triển khai bảo mật đảm bảo an toàn khi sử dụng các phần mềm mua từ các bên uy tín?
- Chúng tôi phải bảo vệ những gì? Trước những ai?
- Công ty không có thông tin quan trọng gì nên không cần phải bảo vệ?
- Bảo đảm an toàn cho các ứng dụng/hệ thống công nghệ thông tin (CNTT) là trách nhiệm của ai?
- Là người đứng đầu, không có chuyên môn về bảo mật an toàn, tôi có thể làm được gì?
- Công ty tôi không có (hoặc chỉ có 1-2) nhân viên CNTT, chưa có chuyên môn về an toàn thông tin thì ai sẽ lo việc bảo đảm an toàn?
- Tôi phải quyết định như thế nào đối với các giải pháp, biện pháp bảo vệ, bảo đảm an toàn từ các đề xuất của nhân viên trong nội bộ hoặc từ bên ngoài?
- Tham vấn hoặc tư vấn ai về ATTT có thể tin tưởng được?
- ? ? ?



Mô hình các lớp bảo đảm an toàn của mọi tổ chức

Dữ liệu và tài sản thông tin quan trọng là mục tiêu cần bảo vệ của Doanh nghiệp, cũng là mục tiêu tấn công của các tổ chức và tội phạm mạng

LÃNH ĐẠO ĐẢM BẢO AN TOÀN THÔNG TIN LÀM NHỮNG GÌ?



- KHÔNG CẦN có chuyên môn về công nghệ thông tin, an toàn thông tin
- Nguyên tắc: ĐẢM BẢO ATTT LÀ THÀNH PHẦN BẮT BUỘC TRONG MỌI HỆ THỐNG THÔNG TIN
- Áp dụng tư duy quản trị và quản trị rủi ro để đảm bảo an toàn
- Đảm bảo an toàn thông tin là kết hợp giữa các biện pháp, giải pháp PHI KỸ THUẬT và KỸ THUẬT, trong đó các biện pháp PHI KỸ THUẬT đóng vai trò quan trọng
- Cần hoạch định triển khai đảm bảo an toàn thông tin của tổ chức mang tính hệ thống, tổng thể; tổ chức thượng tầng để vận hành hạ tầng thuận lợi, duy trì và kiểm soát được
- Thúc đẩy văn hoá an toàn trong tổ chức, trong mỗi nhân viên

TRIỂN KHAI ĐẢM BẢO AN TOÀN THÔNG TIN TỔNG THỂ

Luật và quy định	Chiến lược ATTT	Chính sách ATTT	Nhân lực, nhận thức ATTT	Quản lý rủi ro	Mô hình Quản lý bảo mật	Thực hành bảo mật	Kế hoạch ứng phó	Duy trì bảo mật	Các cơ chế bảo mật (công nghệ)

Giảm rủi ro mất an toàn cho hệ thống thông tin

CÔNG VIỆC CHÍNH CỦA LÃNH ĐẠO DOANH NGHIỆP

1. Tuân thủ các **yêu cầu của luật pháp, ngành và quốc tế**
2. Xây dựng, vận hành **Kế hoạch quản trị và Chiến lược ATTT -** phù hợp với chiến lược hoạt động của tổ chức, của doanh nghiệp:
3. Xây dựng, ban hành, duy trì thực thi hiệu quả **chính sách ATTT**
4. Quản lý, phát triển **Nguồn nhân lực CNTT, ATTT của tổ chức; nâng cao nhận thức ATTT** cho tất cả nhân viên
5. Chỉ đạo triển khai, quản lý và kiểm soát **Rủi ro an toàn thông tin**
6. **Duy trì đảm bảo ATTT** trong mọi hoạt động của tổ chức như quản lý nhân sự, quản lý các thay đổi, đảm bảo ATTT
7. Chuẩn bị và duy trì sẵn sàng **Kế hoạch ứng phó sự cố ATTT**
8. Triển khai **các cơ chế bảo mật cơ bản** cho các hệ thống thông tin

ĐỀ XUẤT TRIỂN KHAI ĐẢM BẢO AN TOÀN ĐỐI VỚI DOANH NGHIỆP

ĐỀ XUẤT CỤ THỂ CHO CÁC DOANH NGHIỆP VỪA VÀ NHỎ

1. **Rà soát các quy định pháp luật có liên quan, đảm bảo tuân thủ**:
   - Việt Nam: Luận An toàn thông tin mạng, Luật An ninh mạng, Nghị định Bảo vệ dữ liệu cá nhân, các quy định của Ngành
   - Quốc tế: các thị trường và khách hàng mà doanh nghiệp đang hướng đến và đang cung cấp SPDV để biết phải tuân thủ các quy định nào. Ví dụ: HIPPA - Hoa Kỳ, GDPR của Liên Minh Châu Âu
2. **Doanh nghiệp cần có chiến lược kinh doanh tầm nhìn** (tối thiểu 5 năm)**, làm cơ sở xây dựng chiến lược bảo đảm an toàn thông tin.** Cụ thể cần đưa ra các mục tiêu an toàn cần đạt được, ví dụ tuân thủ chặt chẽ các quy định, bảo mật và không lộ lọt thông tin khách hàng, bảo mật các bí mật kinh doanh của doanh nghiệp, …

ĐỀ XUẤT CỤ THỂ CHO CÁC DOANH NGHIỆP VỪA VÀ NHỎ

3. **Xây dựng, ban hành và đảm bảo tuân thủ các chính sách an toàn thông tin** của doanh nghiệp.
   - Chính sách ATTT là một tập hợp các "Hướng dẫn của doanh nghiệp quy định hành vi nhất định trong tổ chức về ATTT".
   - Chính sách ATTT dựa trên các mục tiêu chiến lược ATTT
   - Cần xây dựng phù hợp, dễ hiểu, dễ nhớ, dễ áp dụng
   - Áp dụng không chỉ trong nội bộ DN mà cả các bên liên quan
   - Đảm bảo tuân thủ, nhất là người đứng đầu; duy trì, cập nhật
4. **Xây dựng năng lực về con người đảm bảo ATTT của doanh nghiệp:**
   - Có nhân sự kỹ thuật làm việc toàn thời gian / bán thời gian có hiểu biết về ATTT và vận hành triển khai đảm bảo ATTT của DN
   - Nâng cao nhận thức ATTT cho toàn thể nhân viên của DN
   - Thúc đẩy văn hoá an toàn thông tin trong tổ chức

ĐỀ XUẤT CỤ THỂ CHO CÁC DOANH NGHIỆP VỪA VÀ NHỎ

5. **Chỉ đạo triển khai quản lý rủi ro ATTT** của Doanh nghiệp.
   - Lập danh sách và quản lý các tài sản thông tin của doanh nghiệp (con người, quy trình, dữ liệu, thiết bị phần cứng, phần mềm, mạng)
   - Quản lý và kiểm soát các mối đe doạ (Threats) và các điểm yếu (Vulnerabilities) của từng tài sản thông tin
   - Phân loại tài sản thông tin, xác định các ưu tiên
   - Đánh giá tác động của những tài sản thông tin đó với hoạt động kinh doanh của tổ chức
   - Có những biện pháp giảm thiểu và ứng phó với các rủi ro cụ thể
6. **Chuẩn bị kế hoạch ứng phó sự cố ATTT:**
   - Quy trình và các phương án ứng phó cụ thể
   - Lưu ý tính khả thi, và phù hợp với tổ chức
   - Có các hỗ trợ của các tổ chức, chuyên gia bên ngoài ứng phó khi xảy ra sự cố

ĐỀ XUẤT CỤ THỂ CHO CÁC DOANH NGHIỆP VỪA VÀ NHỎ

7. **Chỉ đạo triển khai các giải pháp bảo đảm an toàn cơ bản để bảo vệ cho hệ thống thông tin và các ứng dụng** của Doanh nghiệp.

- Thuê tư vấn lập thiết kế hệ thống thông tin của Công ty phù hợp với hoạt động kinh doanh và chiến lược bảo đảm ATTT của công ty
- Thiết bị tường lửa (firewall) cho mạng kết nối Internet của Công ty
- Thiết bị / giải pháp tường lửa WAF (Web Application Firewal) cho các ứng dụng của công ty
- Giải pháp phát hiện và ngăn chặn mã độc trên các máy chủ, máy tính làm việc
- Nếu các ứng dụng của Công ty triển khai trên nền điện toán đám mây của Nhà cung cấp giải pháp, đề nghị bổ sung giải pháp bảo mật cho ứng dụng và bảo mật dữ liệu khách hàng
- Cân nhắc thuê dịch vụ đảm bảo an toàn cho dữ liệu quan trọng và ứng dụng của Công ty từ bên cung cấp dịch vụ ATTT có uy tín

Trao đổi

Trân trọng Cảm ơn!

Nguyễn Hữu Nguyên
Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam
VNCERT/CC
Cục An toàn thông tin, Bộ Thông tin và Truyền thông
Email: nhnguyen@mic.gov.vn