##### **Phụ lục 1**

##### **Danh sách Nhóm kiến thức, kỹ năng kỹ thuật cơ bản về an toàn thông tin mạng**

*(Ban hành kèm theo thông tư số /2021/TT-BTTTT ngày / /2021 của*

*Bộ trưởng Bộ Thông tin và Truyền thông)*

|  |  |  |
| --- | --- | --- |
| **STT** | **Nội dung/ yêu cầu cần đạt** | **Chi tiết** |
| 1 | **Tổng quan về mạng máy tính, Internet, TCP/IP, DNS,…** | - Kiến thức về kết nối Mạng cục bộ và mạng diện rộng của tổ chức.- Có kiến ​​thức về các thiết bị và chức năng phần cứng mạng.- Kiến thức về các khái niệm viễn thông (ví dụ: Kênh truyền thông, Liên kết hệ thống Lập ngân sách, Hiệu quả phổ, Ghép kênh).- Kiến thức về truyền dữ liệu, tốc độ truyền, băng thông…. - Kiến thức về các khái niệm, thuật ngữ và hoạt động của nhiều loại hình thông tin liên lạc phương tiện truyền thông (máy tính và mạng điện thoại, vệ tinh, cáp quang, không dây).- Kiến thức về các thành phần và kiến ​​trúc máy tính vật lý, bao gồm các chức năng của các thành phần và thiết bị ngoại vi khác nhau (ví dụ: CPU, màn hình, lưu trữ dữ liệu).- Có kiến ​​thức về mô hình OSI. - Có kiến ​​thức về hoạt động cơ bản của máy tính.- Kiến thức về các thiết bị mạng phổ biến và cấu hình của chúng.- Kiến thức về thuật ngữ truyền dữ liệu (ví dụ: giao thức mạng, Ethernet, IP, mã hóa, thiết bị quang học, phương tiện di động).- Kiến thức quản trị mạng.- Kiến thức về giao thức mạng TCP/IP.- Kiến thức về khả năng và ứng dụng của thiết bị mạng bao gồm bộ định tuyến, thiết bị chuyển mạch, cầu nối, máy chủ, phương tiện truyền dẫn và phần cứng liên quan.- Kiến thức về Wi-Fi. |
| 2 | **Kỹ năng lập trình và lập trình an toàn** | - Có kiến ​​thức về ngôn ngữ máy tính cấp thấp.- Kiến thức về các khái niệm, nguyên lý lập trình máy tính, bao gồm cả ngôn ngữ máy tính, lập trình, thử nghiệm, gỡ lỗi và các loại tệp.- Thuần thục chức năng của một số phần mềm ứng dụng thông dụng: Xử lý văn bản, bảng tính, hệ quản trị cơ sở dữ liệu, trình chiếu, thư điện tử, trình duyệt web, biên tập ảnh, trò chơi máy tính và một số phần mềm khác.- Biết khái niệm phần mềm nguồn mở, phân biệt được phần mềm thương mại và phần mềm nguồn mở.- Biết một số chính sách cơ bản về an toàn thông tin và một số văn bản pháp luật về an toàn thông tin của Việt Nam (Luật Luật an toàn thông tin mạng, an ninh mạng,……) . Hiểu tầm quan trọng của việc xây dựng và thi hành chính sách an toàn, an ninh mạng.  |
| 3 | **Lỗ hổng/ điểm yếu ATTT** | - Kiến thức về lỗ hổng ứng dụng.- Có kiến ​​thức về các công cụ, phương pháp và kỹ thuật thiết kế hệ thống bảo mật.- Kiến thức về bảo mật Mạng riêng ảo (VPN).- Kiến thức về phần mềm độc hại. - Kiến thức về lây nhiễm mã độc máy tính/mạng phổ biến (vi rút, Trojan, v.v.) và các phương pháp nhiễm trùng (cổng, tệp đính kèm, v.v.).- Biết các điểm yếu của máy tính cá nhân (lây nhiễm virus và các phần mềm độc hại - malware).- Biết một số biện pháp khắc phục cơ bản những lỗ hổng trên. |
| 4 | **Các kỹ thuật tấn công của tin tặc** | - Biết một số phương thức tấn công mạng chủ yếu của tin tặc (hacker) như trinh sát, dò quét, tấn công vào các điểm yếu, sử dụng các lỗ hổng an toàn. Biết về một số dạng tấn công phổ biến qua mạng Internet chính như tấn công từ chối dịch vụ DOS, DDOS, APT, botnet…..- Biết về các cơ chế và công nghệ chống lại tấn công trên mạng như phân vùng mạng, mạng riêng ảo (VPN), một số hệ thống bảo vệ phổ biến (ví dụ: tường lửa). Hiểu chức năng và giới hạn của tường lửa.- Hiểu các chế độ đảm bảo an toàn của mạng: kiểm soát phần mềm độc, kiểm soát truy nhập trái phép dữ liệu, đảm bảo tính riêng tư (maintaining privacy). - Biết các công nghệ bảo vệ hệ thống cơ bản như đăng nhập, kiểm soát truy nhập, quản trị mật khẩu, quản trị người sử dụng, khai thác tệp tin hồ sơ truy nhập (log). |
| 5 | **Các nguyên lý về an toàn thông tin** | - Có kiến ​​thức về quản trị dữ liệu và các chính sách chuẩn hóa dữ liệu.- Kiến thức về các quy trình quản lý rủi ro.- Kiến thức về an toàn, an ninh mạng và các nguyên tắc riêng tư.- Kiến thức về các mối đe dọa và lỗ hổng không gian mạng.- Kiến thức về các nguyên tắc và khái niệm mạng cục bộ và mạng diện rộng bao gồm cả quản lý băng thông. |
| 6 | **An toàn các giao thức mạng** | - Kiến thức về các giao thức mạng và định tuyến phổ biến (ví dụ: TCP / IP), các dịch vụ (ví dụ: web, thư, DNS) và cách chúng tương tác để cung cấp thông tin liên lạc qua mạng.- Kiến thức về các khái niệm và giao thức mạng máy tính và bảo mật mạng. |
| 7 | **An toàn ứng dụng và các dịch vụ mạng** | - Kiến thức về các dịch vụ mạng và giao thức tương tác cung cấp mạng thông tin liên lạc.- Kiến thức về các ứng dụng phần mềm cơ bản (ví dụ: lưu trữ và sao lưu dữ liệu, cơ sở dữ liệu ứng dụng) và các loại lỗ hổng đã được tìm thấy trong các ứng dụng đó.- Kiến thức về các dịch vụ web (ví dụ: kiến ​​trúc hướng dịch vụ, Truy cập đối tượng đơn giản Giao thức và ngôn ngữ mô tả dịch vụ web). |
| 8 | **An toàn cho máy chủ và hệ thống và thiết bị.** | - Kiến thức về cơ chế kiểm soát truy cập máy chủ/mạng (ví dụ: danh sách kiểm soát truy cập, các khả năng)- Kiến thức về quản trị máy chủ và các lý thuyết, khái niệm về kỹ thuật hệ thống và các phương pháp.- Có kiến ​​thức về hệ điều hành máy chủ và máy khách.- Có kiến ​​thức về các khái niệm quản trị hệ thống.- Kiến thức về các loại trang web, quản trị, chức năng và hệ thống quản lý nội dung.- Kiến thức về các khái niệm liên quan đến trang web (ví dụ: máy chủ/trang web, lưu trữ, DNS, đăng ký, ngôn ngữ web như HTML).- Kiến thức về cấu trúc và nội bộ của hệ điều hành Unix / Linux và Windows (ví dụ: quản lý tiến trình, cấu trúc thư mục, các ứng dụng đã cài đặt).- Có kiến ​​thức về hệ điều hành.- Có kiến thức về quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ;- Có kiến thức về cập nhật; sao lưu dự phòng và khôi phục sau khi xảy ra sự cố.- Kiến thức về các khái niệm và chức năng của tường lửa ứng dụng (ví dụ: Điểm đơn của xác thực/kiểm toán/thực thi chính sách, quét tin nhắn cho nội dung độc hại, dữ liệu ẩn danh để tuân thủ PCI và PII, quét bảo vệ mất dữ liệu, được tăng tốc hoạt động mật mã, bảo mật SSL, xử lý REST / JSON).- Kiến thức về các thiết bị điện tử (ví dụ: hệ thống/linh kiện máy tính, kiểm soát truy cập thiết bị, máy ảnh kỹ thuật số, máy quét kỹ thuật số, máy tổ chức điện tử, ổ cứng, thẻ nhớ, modem, thành phần mạng, thiết bị được nối mạng, thiết bị điều khiển gia đình được nối mạng, máy in, thiết bị lưu trữ di động, điện thoại, máy photocopy, máy fax, v.v.).- Kiến thức về kỹ thuật phần cứng được áp dụng cho kiến ​​trúc máy tính (ví dụ: mạch bo mạch, bộ xử lý, chip và phần cứng máy tính). |
| 9 | **Con người và Chính sách quản lý an toàn thông tin** | - Kiến thức về các chính sách bảo mật người dùng của tổ chức công nghệ thông tin (CNTT) (ví dụ: tạo tài khoản, quy tắc mật khẩu, kiểm soát truy cập).- Kiến thức về chính sách, quy trình Quản lý an toàn mạng; Quản lý an toàn máy chủ và ứng dụng; Quản lý an toàn dữ liệu; Quản lý sự cố an toàn thông tin; quản lý an toàn người sử dụng đầu cuối |
| 10 | **Các tiêu chuẩn an toàn thông tin** | - TCVN ISO/IEC 27001:2009 Công nghệ thông tin - Hệ thống quản lý an toàn thông tin - Các yêu cầu- TCVN ISO/IEC 27002:2011 Công nghệ thông tin - Các kỹ thuật an toàn - Quy tắc thực hành Quản lý an toàn thông tin- TCVN 8709-1:2011 ISO/IEC 15408-1:2009 Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT- Phần 1: Giới thiệu và mô hình tổng quát- TCVN 8709-2:2011 ISO/IEC 15408-2:2008 Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT- Phần 2: Các thành phần chức năng an toàn- TCVN 8709-3:2011 ISO/IEC 15408-3:2008 Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT- Phần 3: Các thành phần đảm bảo an toàn- TCVN 10295:2014 ISO/IEC 27005:2011 Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý rủi ro an toàn thông tin- TCVN 10541:2014 ISO/IEC 27003:2010 Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn triển khai hệ thống quản lý an toàn thông tin- TCVN 10543:2014 ISO/IEC 27010:2012 Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý an toàn trao đổi thông tin liên tổ chức, liên ngành- TCVN 9801-3:2014 ISO/IEC 27033-3:2010 Công nghệ thông tin - Kỹ thuật an toàn - An toàn mạng - Phần 3: Các kịch bản kết nối mạng tham chiếu - Nguy cơ, kỹ thuật thiết kế và các vấn đề kiểm soát- TCVN 9801-2:2015 Công nghệ thông tin - Các kỹ thuật an toàn - An toàn mạng - Phần 2: Hướng dẫn thiết kế và triển khai an toàn mạng- TCVN 11238:2015 Công nghệ thông tin - Các kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Tổng quan và từ vựng- TCVN 11239:2015 Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý sự cố an toàn thông tin- TCVN 11386:2016 Công nghệ thông tin - Các kỹ thuật an toàn - Phương pháp đánh giá an toàn công nghệ thông tin.- TCVN 11393-1:2016 ISO/IEC 13888-1:2009 Công nghệ thông tin - Các kỹ thuật an toàn - Chống chối bỏ - Phần 1: Tổng quan- TCVN ISO/IEC 11930:2017. |