Khái niệm - an toàn và bảo mật

An toàn và bảo mật hệ thống thông tin (Trường Đại học Kinh tế, Đại học Đà Nẵng)

Khái niệm	Định nghĩa	Ví dụ cụ thể
Mối đe dọa (Threat)	Một yếu tố bên ngoài có khả năng gây thiệt hại hoặc tấn công hệ thống.	Tin tặc xâm nhập vào hệ thống nhằm mục đích đánh cắp dữ liệu.
Điểm yếu (Weakness)	Một khía cạnh nội tại của hệ thống cho phép mối đe dọa có thể xâm nhập.	Hệ thống chưa được cập nhật bản vá bảo mật mới nhất.
Lỗ hổng (Vulnerability)	Một điểm yếu cụ thể trong phần mềm hoặc hệ thống mà kẻ tấn công có thể khai thác.	Một lỗ hổng SQL injection trong ứng dụng web cho phép truy cập cơ sở dữ liệu.
Rủi ro (Risk)	Khả năng xảy ra thiệt hại do mối đe dọa gây ra, thường được đánh giá dựa trên xác suất và tác động.	Xác suất một lỗ hổng bảo mật bị khai thác dẫn đến việc mất dữ liệu quan trọng cho tổ chức.

Hệ điều hành	Mối đe dọa (Threat)	Điểm yếu (Weakness)	Lỗ hổng (Vulnerability)	Rủi ro (Risk)
Windows 8	Tin tặc sử dụng malware để truy cập trái phép	Hệ thống chưa được cập nhật phiên bản mới nhất	Lỗ hổng trong Internet Explorer cho phép khai thác từ xa	Dữ liệu nhạy cảm có thể bị đánh cắp hoặc hủy hoại
Windows 10	Tấn công phishing nhằm vào người dùng	Thiếu kiến thức bảo mật của người dùng	Lỗ hổng trong hệ thống xác thực Windows Authenticator	Nếu bị tấn công, tài

Hệ điều hành	Mối đe dọa (Threat)	Điểm yếu (Weakness)	Lỗ hổng (Vulnerability)	Rủi ro (Risk)
				khoản người dùng có thể bị chiếm đoạt
Windows 11	Ransomware mã hóa dữ liệu người dùng	Quá trình cập nhật không tự động	Lỗ hổng trong Microsoft Defender có thể cho phép tấn công	Công ty có thể bị gián đoạn hoạt động và mất dữ liệu

Mối đe dọa/ nguy cơ (threat): Mối đe dọa là bất kỳ một hành động nào có thể gây hư hại đến các tài nguyên hệ thống (gồm phần cứng, phần mềm, CSDL, các file, dữ liệu, hoặc hạ tầng mạng vật lý,…).

❑ Điểm yếu (weakness): là những khiếm khuyết hoặc lỗi tồn tại trọng hệ thống: ▪ Điểm yếu phần cứng ▪ Điểm yếu phần mềm (Hệ điều hành và ứng dụng)

❑ Lỗ hổng (vulnerability): là bất kỳ điểm yếu nào trong hệ thống cho phép mối đe dọa có thể gây tác hại.

Rủi ro (risk): là tiềm năng một mối đe dọa có thể khai khác một lỗ hổng để tấn công hoặc gây nguy hiểm cho hệ thống. Nguy cơ xuất hiện khi có mối đe dọa và lỗ hổng bảo mật.

Quan hệ giữa Mối đe dọa và Lỗ hổng: ➢ Các mối đe dọa thường khai thác một hoặc một số lỗ hổng đã biết để thực hiện các cuộc tấn công phá hoại; ➢ Nếu tồn tại một lỗ hổng trong hệ thống, sẽ có khả năng một mối đe dọa trở thành hiện thực; ➢ Không thể triệt tiêu được hết các mối đe dọa, nhưng có thể giảm thiểu các lỗ hổng, qua đó giảm thiểu khả năng bị tận dụng để tấn công

Khái niệm	Định nghĩa	Ví dụ cụ thể
Mối đe dọa	Các yếu tố bên ngoài có thể gây hại cho hệ thống hoặc tài sản.	Một nhóm tội phạm mạng có thể tấn công vào hệ thống máy tính của công ty để đánh cắp dữ liệu khách hàng.
Điểm yếu	Các yếu tố bên trong hoặc đặc điểm của hệ thống có thể bị khai thác bởi mối đe dọa.	Phần mềm của công ty không được cập nhật và vá lỗi thường xuyên, tạo cơ hội cho phần mềm độc hại xâm nhập.
Lỗ hổng	Những thiếu sót cụ thể trong hệ thống hoặc quy trình cho phép mối đe dọa xâm nhập.	Một lỗ hổng bảo mật trong ứng dụng web cho phép kẻ tấn công thực hiện tấn công SQL injection để truy cập dữ liệu nhạy cảm.
Rủi ro	Kết quả có thể xảy ra khi một mối đe dọa khai thác lỗ hổng và gây ra điểm yếu.	Nếu kẻ tấn công xâm nhập vào hệ thống qua lỗ hổng bảo mật, công ty có thể đối mặt với mất dữ liệu khách hàng và tổn thất tài chính.

Ví dụ tổng hợp:

1. **Mối đe dọa**: Kẻ tấn công mạng.
2. **Điểm yếu**: Hệ thống bảo mật yếu kém.
3. **Lỗ hổng**: Phần mềm chưa được cập nhật với bản vá bảo mật mới nhất.
4. **Rủi ro**: Kẻ tấn công có thể xâm nhập vào hệ thống, gây ra sự rò rỉ dữ liệu và tổn thất tài chính cho công ty.

Hy vọng bảng so sánh này giúp làm rõ sự khác biệt và mối liên hệ giữa các khái niệm!

Không chia sẻ thông tin nhạy cảm. Các đoạn chat có thể được xem xét và sử dụng để huấn luyện các mô hình của chúng tôi. Tìm hiểu thêm

---

Khái niệm	Đặc điểm	Ví dụ cụ thể
Mối đe dọa (Threat)	- Yếu tố bên ngoài có khả năng gây hại. - Không phải lúc nào cũng có thể kiểm soát. - Có thể là hành vi hoặc sự kiện.	Một hacker có thể tấn công hệ thống mạng của công ty để lấy cắp thông tin tài chính.
Điểm yếu (Weakness)	- Yếu tố nội bộ hoặc đặc điểm của hệ thống. - Có thể là sự thiếu sót trong thiết kế, quy trình, hoặc thực hành. - Có thể được cải thiện hoặc khắc phục.	Chính sách bảo mật của công ty không bao gồm việc mã hóa dữ liệu khi truyền tải, làm giảm mức độ bảo vệ thông tin nhạy cảm.
Lỗ hổng	- Các thiếu sót hoặc lỗi cụ	Một lỗi trong phần mềm quản lý khách

	thể trong hệ thống. - Là cơ hội cho mối đe dọa khai thác. - Có thể là lỗi phần mềm, cấu hình sai, hoặc thiếu biện pháp bảo vệ.	hàng cho phép truy cập không cần quyền hạn vào dữ liệu cá nhân của khách hàng.
Rủi ro (Risk)	- Kết quả có thể xảy ra khi mối đe dọa khai thác lỗ hổng và điểm yếu. - Là sự kết hợp của khả năng xảy ra sự kiện và tác động của nó. - Có thể quản lý bằng các biện pháp giảm thiểu.	Nếu lỗ hổng bảo mật trong phần mềm quản lý khách hàng bị khai thác bởi hacker, có thể dẫn đến việc rò rỉ dữ liệu khách hàng và tổn thất tài chính.

Khái niệm	Đặc điểm & Tính năng	Ví dụ cụ thể
Mối đe dọa (Threat)	- **Đặc điểm**: Yếu tố bên ngoài có thể gây hại. - **Tính năng**: Có thể là hành động, sự kiện, hoặc điều kiện không mong muốn. - **Kiểm soát**: Khó kiểm soát hoàn toàn.	Một tổ chức khủng bố có thể tấn công mạng vào cơ sở hạ tầng quan trọng để gây gián đoạn dịch vụ công cộng.
Điểm yếu (Weakness)	- **Đặc điểm**: Các yếu tố nội bộ có thể dẫn đến tổn thất nếu bị khai thác. - **Tính năng**: Có thể là quy trình, chính sách, hoặc cấu hình không tối ưu. - **Kiểm soát**: Có thể được cải thiện thông qua các biện pháp bảo mật.	Công ty không thường xuyên kiểm tra và cập nhật các chính sách bảo mật, dẫn đến việc sử dụng các biện pháp bảo mật lỗi thời.
Lỗ hổng (Vulnerability)	- **Đặc điểm**: Lỗi hoặc thiếu sót trong hệ thống có thể bị khai thác. - **Tính năng**: Có thể là lỗi phần mềm, cấu hình sai, hoặc thiếu sót trong thiết kế. - **Kiểm soát**: Có thể phát	Một phần mềm có lỗi bảo mật cho phép tấn công SQL injection, khiến dữ liệu trong cơ sở dữ liệu có thể bị truy cập trái phép.

Khái niệm	Đặc điểm & Tính năng	Ví dụ cụ thể
	hiện và vá lỗi nếu được kiểm tra thường xuyên. - **Đặc điểm**: Kết quả tiềm ẩn từ việc mối đe dọa khai thác lỗ hổng và điểm yếu. - **Tính năng**: Phản ánh khả năng xảy ra và tác động của sự kiện không mong muốn. - **Kiểm soát**: Có thể giảm thiểu bằng cách thực hiện các biện pháp quản lý rủi ro.	
Rủi ro (Risk)		Nếu lỗ hổng bảo mật trong phần mềm quản lý khách hàng bị khai thác, có thể dẫn đến việc rò rỉ dữ liệu khách hàng và gây thiệt hại tài chính lớn cho công ty.

Ví dụ cụ thể:

1. **Mối đe dọa (Threat)**:
   - **Đặc điểm**: Kẻ tấn công mạng.
   - **Tính năng**: Có khả năng tấn công vào hệ thống và làm hỏng hoặc lấy cắp dữ liệu.
   - **Ví dụ**: Một nhóm hacker có thể thực hiện tấn công ransomware để mã hóa dữ liệu của công ty và yêu cầu tiền chuộc.
2. **Điểm yếu (Weakness)**:
   - **Đặc điểm**: Chính sách bảo mật không đầy đủ.
   - **Tính năng**: Có thể tạo cơ hội cho các mối đe dọa khai thác.
   - **Ví dụ**: Chính sách quản lý mật khẩu của công ty không yêu cầu mật khẩu phức tạp và thay đổi định kỳ.
3. **Lỗ hổng (Vulnerability)**:
   - **Đặc điểm**: Lỗi trong phần mềm.
   - **Tính năng**: Cung cấp lối vào cho các cuộc tấn công nếu không được xử lý.
   - **Ví dụ**: Một lỗ hổng trong phần mềm email cho phép kẻ tấn công thực hiện tấn công phishing để lấy cắp thông tin đăng nhập.
4. **Rủi ro (Risk)**:
   - **Đặc điểm**: Kết quả từ việc khai thác điểm yếu và lỗ hổng.
   - **Tính năng**: Có thể dẫn đến thiệt hại và tổn thất nếu không được quản lý.
   - **Ví dụ**: Nếu lỗ hổng bảo mật trong phần mềm email bị khai thác, công ty có thể đối mặt với mất dữ liệu nhạy cảm và tổn thất uy tín.

Đặc điểm/Tính năng	Mối đe dọa (Threat)	Điểm yếu (Weakness)	Lỗ hổng (Vulnerability)	Rủi ro (Risk)
Nguồn gốc	Bên ngoài hoặc bên trong tổ chức	Bên trong tổ chức	Bên trong hoặc bên ngoài tổ chức	Bên trong hoặc bên ngoài tổ chức
Ví dụ	- Hacker tấn công hệ thống mạng - Thiên tai như lũ lụt, cháy rừng	- Mật khẩu yếu, dễ đoán - Thiếu quy trình quản lý bảo mật	- Lỗ hổng bảo mật trong phần mềm - Quy trình xác thực yếu	- Thiệt hại danh tiếng và tài chính do bị tấn công - Mất dữ liệu quan trọng do sự cố hệ thống
Khả năng xảy ra	Không thể dự đoán hoàn toàn	Có thể dự đoán và kiểm soát	Có thể dự đoán và kiểm soát	Có thể ước tính và quản lý
Tác động	Nghiêm trọng, có thể ảnh hưởng đến hoạt động, uy tín và tài chính của tổ chức	Có thể gây ảnh hưởng đến hoạt động của tổ chức	Có thể gây ra thiệt hại nếu bị khai thác	Phụ thuộc vào xác suất và mức độ tác động của mối đe dọa
Cách giải quyết	Phải có biện pháp bảo vệ và ứng phó thích hợp	Cần khắc phục và loại bỏ điểm yếu	Cần vá lỗi và triển khai các biện pháp bảo mật	Cần đánh giá, lập kế hoạch và quản lý rủi ro

Windows 8:

- Mối đe dọa: Các phần mềm độc hại như mã độc ransomware có thể tấn công vào các hệ thống Windows 8 chưa được cập nhật bảo mật.
- Điểm yếu: Nhiều người dùng phàn nàn về giao diện mới "Metro" của Windows 8, khiến họ khó sử dụng và làm việc.

- Lỗ hổng: Các lỗ hổng bảo mật trong trình duyệt Internet Explorer trên Windows 8 có thể cho phép hacker đánh cắp thông tin.
- Rủi ro: Nếu hệ thống Windows 8 bị nhiễm mã độc, dữ liệu quan trọng có thể bị mã hóa và yêu cầu tiền chuộc để giải mã.

Windows 10:

- Mối đe dọa: Các cuộc tấn công lừa đảo qua email nhằm vào người dùng Windows 10 để trộm thông tin đăng nhập.
- Điểm yếu: Một số người dùng phàn nàn về việc Windows 10 tự động cập nhật mà không có sự đồng ý của họ.
- Lỗ hổng: Các lỗ hổng bảo mật trong Windows Defender trên Windows 10 có thể cho phép hacker thực hiện các cuộc tấn công.
- Rủi ro: Nếu hệ thống Windows 10 bị nhiễm mã độc, dữ liệu và thông tin cá nhân của người dùng có thể bị đánh cắp.

Windows 11:

- Mối đe dọa: Các nhóm tin tặc có thể tấn công vào các hệ thống Windows 11 chưa được cập nhật bảo mật.
- Điểm yếu: Một số người dùng phàn nàn về giao diện mới của Windows 11, khiến họ khó làm quen và sử dụng.
- Lỗ hổng: Các lỗ hổng bảo mật trong Driver Update của Windows 11 có thể cho phép hacker truy cập vào hệ thống.
- Rủi ro: Nếu hệ thống Windows 11 bị nhiễm mã độc, hoạt động kinh doanh của doanh nghiệp có thể bị gián đoạn nghiêm trọng.

Khái niệm	Đặc điểm & Tính năng	Ví dụ cụ thể với Windows 8, Windows 10, Windows 11
Mối đe dọa (Threat)	- **Đặc điểm**: Yếu tố bên ngoài có khả năng gây hại. - **Tính năng**: Có thể là hành động hoặc sự kiện không mong muốn. - **Kiểm soát**: Khó kiểm soát hoàn toàn.	**Windows 8, 10, 11**: Một cuộc tấn công từ nhóm hacker sử dụng mã độc hoặc phần mềm độc hại để xâm nhập vào hệ thống của người dùng, có thể nhằm lấy cắp dữ liệu hoặc làm gián đoạn hoạt động.
Điểm yếu (Weakness)	- **Đặc điểm**: Các yếu tố nội bộ có thể dẫn đến tổn thất nếu bị khai thác. - **Tính năng**: Có thể là quy trình, chính sách, hoặc cấu hình không tối ưu. - **Kiểm soát**: Có thể	**Windows 8**: Cấu hình mặc định cho phép chia sẻ tập tin qua mạng mà không yêu cầu bảo mật cao. Điều này có thể tạo điều kiện cho việc truy cập trái phép vào các tài liệu nhạy cảm trên mạng nội bộ.

	được cải thiện thông qua các biện pháp bảo mật.	
Lỗ hổng (Vulnerability)	- **Đặc điểm**: Lỗi hoặc thiếu sót trong hệ thống có thể bị khai thác. - **Tính năng**: Có thể là lỗi phần mềm, cấu hình sai, hoặc thiếu sót trong thiết kế. - **Kiểm soát**: Có thể phát hiện và vá lỗi nếu được kiểm tra thường xuyên.	**Windows 10**: Lỗi bảo mật "BlueKeep" (CVE-2019-0708) ảnh hưởng đến Remote Desktop Services, cho phép kẻ tấn công thực hiện tấn công từ xa mà không cần xác thực, gây ra nguy cơ cao về tấn công từ xa.
Rủi ro (Risk)	- **Đặc điểm**: Kết quả tiềm ẩn từ việc mối đe dọa khai thác lỗ hổng và điểm yếu. - **Tính năng**: Phản ánh khả năng xảy ra và tác động của sự kiện không mong muốn. - **Kiểm soát**: Có thể giảm thiểu bằng cách thực hiện các biện pháp quản lý rủi ro.	**Windows 11**: Nếu lỗ hổng bảo mật tương tự như "PrintNightmare" (CVE-2021-34527) không được khắc phục, kẻ tấn công có thể khai thác để có quyền truy cập hệ thống, dẫn đến mất dữ liệu nhạy cảm và thiệt hại tài chính cho người dùng.

hái niệm	**Đặc điểm & Tính năng**	**Ví dụ cụ thể với Windows 8**
Mối đe dọa (Threat)	- **Đặc điểm**: Yếu tố bên ngoài có khả năng gây hại. - **Tính năng**: Có thể là hành động hoặc sự kiện không mong muốn. - **Kiểm soát**: Khó kiểm soát hoàn toàn.	**Windows 8**: Một cuộc tấn công từ nhóm hacker sử dụng phần mềm độc hại (malware) để xâm nhập vào máy tính của người dùng nhằm lấy cắp thông tin cá nhân.
Điểm yếu (Weakness)	- **Đặc điểm**: Các yếu tố nội bộ có thể dẫn đến	**Windows 8**: Tính năng chia sẻ tệp qua mạng mặc định có thể không yêu cầu xác thực mạnh

	tổn thất nếu bị khai thác. - **Tính năng**: Có thể là quy trình, chính sách, hoặc cấu hình không tối ưu. - **Kiểm soát**: Có thể được cải thiện thông qua các biện pháp bảo mật.	mẽ, tạo cơ hội cho việc truy cập trái phép vào các tài liệu nhạy cảm.
Lỗ hổng (Vulnerability)	- **Đặc điểm**: Lỗi hoặc thiếu sót trong hệ thống có thể bị khai thác. - **Tính năng**: Có thể là lỗi phần mềm, cấu hình sai, hoặc thiếu sót trong thiết kế. - **Kiểm soát**: Có thể phát hiện và vá lỗi nếu được kiểm tra thường xuyên.	**Windows 8**: Lỗi bảo mật "CVE-2012-0156" trong Internet Explorer 10 cho phép kẻ tấn công thực thi mã từ xa qua lỗ hổng trong trình duyệt.
Rủi ro (Risk)	- **Đặc điểm**: Kết quả tiềm ẩn từ việc mối đe dọa khai thác lỗ hổng và điểm yếu. - **Tính năng**: Phản ánh khả năng xảy ra và tác động của sự kiện không mong muốn. - **Kiểm soát**: Có thể giảm thiểu bằng cách thực hiện các biện pháp quản lý rủi ro.	**Windows 8**: Nếu lỗ hổng "CVE-2012-0156" trong Internet Explorer không được vá, kẻ tấn công có thể khai thác lỗ hổng để cài đặt phần mềm độc hại trên máy tính, gây mất dữ liệu và thiệt hại tài chính cho người dùng.

1. Mối đe dọa:
    - Các phần mềm độc hại như mã độc ransomware có thể tấn công vào các hệ thống Windows 8 chưa được cập nhật bảo mật. Ví dụ, WannaCry là một loại mã độc ransomware đã tấn công nhiều hệ thống Windows 8 chưa được vá lỗi.
2. Điểm yếu:
    - Giao diện "Metro" mới của Windows 8 gây nhiều tranh cãi, nhiều người dùng phàn nàn về việc khó sử dụng và làm việc so với giao diện truyền thống của Windows 7. Ví dụ, nhiều

người cảm thấy khó tìm kiếm và mở các ứng dụng trên màn hình khởi động.

3. Lỗ hổng:
    - Các lỗ hổng bảo mật trong trình duyệt Internet Explorer trên Windows 8 có thể cho phép hacker đánh cắp thông tin người dùng. Ví dụ, lỗ hổng CVE-2013-1300 trong IE10 trên Windows 8 đã được các nhóm tin tặc lợi dụng để thực hiện các cuộc tấn công xâm nhập.
4. Rủi ro:
    - Nếu hệ thống Windows 8 bị nhiễm mã độc, dữ liệu quan trọng có thể bị mã hóa và yêu cầu tiền chuộc để giải mã. Ví dụ, CryptoLocker là một loại mã độc ransomware đã tấn công nhiều máy tính chạy Windows 8, làm người dùng phải trả tiền chuộc để khôi phục dữ liệu.

Hy vọng những ví dụ này sẽ giúp bạn hiểu rõ hơn về các mối đe dọa, điểm yếu, lỗ hổng và rủi ro liên quan đến hệ điều hành Windows 8. Nếu bạn có câu hỏi gì khác, hãy cứ hỏi!