**BÀI TẬP TUẦN 1**

**Họ và tên: Lê Quang Nam**

**MSSV: 1712603**

**Câu 1. Khảo sát và nêu các tác hại cụ thể của việc hư hỏng mất mát dữ liệu trong những năm gần đây?**

**Sự cố của việc hư hỏng và mất mát dữ liệu trong những năm gần đây đang là chủ đề nóng của các doanh nghiệp, tập đoàn cũng như các tổ chức nhà nước. Việc làm hư hỏng mất mát dữ liệu gây thiệt hại lớn về tiền bạc cũng như rò rĩ thông tin khách hàng.**

* **Việc mất mát dữ liệu có chủ đích từ các doanh nghiệp/tập đoàn như bị tấn công bởi virus độc hại, virus tống tiền, Trojans, Malware, hacking hoặc nhân viên bị mua chuộc từ các thế lực thù địch, tấn công phá hoại từ bên ngoài hoặc có thể là do cạnh tranh không lành mạnh. Tác hại của việc mất mát dữ liệu kiểu này thường gây thiệt hại rất lớn cho doanh nghiệp, làm tổn hại đến uy tín, chất lượng của doanh nghiệp. Điển hình như khảo sát năm 2016 của Kaspersky Lab thì tỉ lệ các doanh nghiệp tham gia khảo sát bị tấn công có chủ đích chiếm 49% và 50% doanh nghiệp đối mặt với ransomware. [1]**
* **Việc mất mát dữ liệu do vô ý cũng gây thiệt hại lớn cho cá nhân, doanh nghiệp cũng như tổ chức nhà nước. Một số lỗi dễ gây thiệt hại mất mát hư hỏng dữ liệu như: đăng tải nhầm file, cấu hình tổ chức phương thức sai tiêu chuẩn, nhân viên bị mất máy tính, cấp sai quyền cũng như là mã hóa sai các thông tin quan trọng. Việc rò rĩ, mất mát dữ liệu này cũng gây thiệt hại lớn. Có đến 48% doanh nghiệp bị mất mát dữ liệu do gặp phải lỗi không tuân thủ chính sách liên quan đến quản lý và bảo mật dữ liệu thông qua cuộc khảo sát 100 doanh nghiệp của Việt Nam về vấn đề rò rĩ mất mát dữ liệu năm 2011. [2]**
* **Trong 1 khảo sát năm 2019 của Công ty Công nghệ dữ liệu Acronis (trụ sở chính tại Thụy Sĩ), có tới 65.1% người dùng hoặc thành viên trong gia đình của họ đã từng bị mất mát dữ liệu do xóa nhầm, lỗi phần cứng hay sự cố phần mềm, tăng 29,4% so với năm 2018. Tuy nhiên, đây là lần đầu tiên trong 4 năm khảo sát của hãng, gần như tất cả người dùng (92,7%) đã sao lưu dữ liệu, tăng 24,1% so với năm 2018 và là mức tăng trưởng lớn nhất trong các năm. Có ít hơn một nửa số người dùng nhận thức được nguy cơ của các cuộc tấn công trực tuyến có thể đe dọa các dữ liệu của họ, như tấn công mã độc tống tiền (46%), mã độc đào tiền ảo (53%) và kỹ nghệ xã hội (52%). Việc đào tạo, phổ biến về những mối đe dọa này dường như còn chậm, vì số người dùng biết về mã độc tống tiền chỉ tăng 4% so với năm 2018. [3]**

**Câu 2: Liệt kê 5 tình huống hư hỏng mất mát thông tin cá nhân có gây thiệt hại, cách ngăn ngừa /khắc phục tương ứng?**

* **Tình huống 1: Việc cá nhân tải phần mềm về sử dụng nhưng không tải ở các nguồn chính thống mà tải ở những trang web không chính thống, hoặc có thể là do phần mềm này tính phí nhưng cá nhân không muốn trả phí và tải cr@ck để trải nghiệm hoặc sử dụng cho mục đích cá nhân. Việc tải phần mềm cũng như các tập tin ở những nguồn không chính thống sẽ là cơ hội cho những kẻ tống tiền kẹp thêm 1 số virus độc hại gây phá hủy các dữ liệu trong máy tính cá nhân, 1 số khác sẽ chèn thêm ransomware, trojans mã hóa dữ liệu cá nhân của người tải, sau đó nhắn tin đe dọa, tống tiền thì mới giải mã trả lại dữ liệu. Cách ngăn ngừa và khắc phục là tải phần mềm, tập tin ở những trang chính thống, có sự uy tín trong lĩnh vực mạng và trả phí.**
* **Tình huống 2: Cùng với việc xã hội phát triển thì việc liên lạc, giải trí thông qua các trang mạng xã hội đang rất phát triển, cùng với việc phát triển đó thì lại xuất hiện các phương thức đánh cắp, rò rĩ thông tin cá nhân. Ví dụ như khi chúng ta sử dụng Facebook, việc tò mò về 1 sự kiện gì đó đang nổi trên mạng xã hội khiến chúng ta muốn tìm hiểu sự kiện đó 1 cách nhanh chóng, đây là lúc những tin tặc ra tay. Chúng sẽ tạo những HyperLink sau đó lồng vào các comments trong các bài đăng, việc tò mò và ấn vào link đó sẽ làm chúng ta rò rĩ các thông tin quan trọng. Việc rò rĩ này có thể gây ra việc mất quyền kiểm soát tài khoản, bị xóa những dữ liệu quan trọng được lưu ở cloud, giả danh, cũng như việc bị bán thông tin cho các tổ chức xấu.**
* **Tình huống 3: Việc đánh cắp thông tin cá nhân, thẻ ngân hàng, các tiện ích lưu trong các thiết bị điện tử do việc bị đánh cắp, mất, cướp giật. Việc sử dụng các thiết bị điện tử có độ bảo mật thông tin cao sẽ hạn chế việc bị bẻ khóa, còn đối với các thiết bị điện tử có tính bảo mật kém như các dòng điện thoại cũ, các thiết bị smartphone giá rẻ sẽ làm tăng nguy cơ bị xâm nhập từ các phần mềm thứ 3 giúp việc bẻ khóa điện thoại 1 cách dễ dàng. Khi bị bẻ khóa thì mọi dữ liệu được lưu trong máy sẽ bị đánh cắp, kể cả số tiền trong E-banking. Vì vậy để ngăn ngừa và khắc phục tình huống trên chúng ta cần sử dụng các thiết bị bảo mật thông tin, khó bị bẻ khóa, không nên dùng sim sử dụng phương thức OTP trên chính thiết bị đó, thay vào đó sử dụng 1 thiết bị khác để gửi mã OTP. Sử dụng thiết bị 1 cách an toàn tránh sơ hở để cho các cá nhân xấu có cơ hội hành động.**
* **Tình huống 4: Hiện nay việc 1 trang mạng xã hội phổ biến trên nhiều nền tảng ứng dụng khác nhau, cũng như việc liên kết tài khoản bằng việc đăng nhập bằng 1 lần nhấn thay vì đăng nhập/ đăng ký như bình thường đang khá phổ biến. Tình huống này trang web đăng nhập cần liên kết đến mạng xã hội và yêu cầu 1 số lượng thông tin dữ liệu cần thiết để có thể đăng nhập. Từ đó lợi dụng việc tiện lợi từ việc đăng nhập qua 1 lần nhấn, những kẻ đánh cắp dữ liệu sẽ cố gắng yêu cầu nhiều quyền nhất có thể, ví dụ như có thể đăng bài, share bài viết lên trên profile của trang mạng xã hội bạn đang dùng để đăng nhập. Việc rò rĩ dữ liệu này có nhiều cách khắc phục và ngăn chặn, hạn chế các quyền được yêu cầu, đăng nhập theo cách truyền thống,…**
* **Tình huống 5: Xóa nhầm file quan trọng, ghi đè lên các tập tin quan trọng do bị trùng tên file, hoặc format nhầm ổ đĩa, phân vùng bị lỗi. Việc này gây ra tổn thất dữ liệu quan trọng, gây mất mát dữ liệu. Các cách khắc phục/ ngăn ngừa phổ biến như dùng các phần mềm thứ 3 hỗ trợ việc cứu dữ liệu như: CD Recovery Toolbox, Disk Drill, Recuva…, hạn chế xóa file bằng cách xóa trực tiếp, thay vào đó là xóa gián tiếp và gửi chúng vào TrashBin để có thể recovery 1 cách dễ dàng.**

**CHÚ THÍCH/ THAM KHẢO:**

**[1]: Tạp chí Tài chính điện tử. 2022. 43% doanh nghiệp bị mất dữ liệu sau một cuộc tấn công có chủ đích.** [**http://www.taichinhdientu.vn/bao-mat/43-doanh-nghiep-bi-mat-du-lieu-sau-mot-cuoc-tan-cong-co-chu-dich-155746.html**](http://www.taichinhdientu.vn/bao-mat/43-doanh-nghiep-bi-mat-du-lieu-sau-mot-cuoc-tan-cong-co-chu-dich-155746.html)

**[2] VietnamPlus. 2022. Có 94% doanh nghiệp ở Việt Nam từng mất dữ liệu | Công nghệ | Vietnam+ (VietnamPlus)** [**https://www.vietnamplus.vn/co-94-doanh-nghiep-o-viet-nam-tung-mat-du-lieu/161067.vnp**](https://www.vietnamplus.vn/co-94-doanh-nghiep-o-viet-nam-tung-mat-du-lieu/161067.vnp)

**[3] Tin, A., 2022. Người dùng vẫn mất dữ liệu dù phần lớn đã chủ động sao lưu dữ liệu - An Toàn Thông Tin.** [**http://m.antoanthongtin.gov.vn/lo-hong-attt/nguoi-dung-van-mat-du-lieu-du-phan-lon-da-chu-dong-sao-luu-du-lieu-105190**](http://m.antoanthongtin.gov.vn/lo-hong-attt/nguoi-dung-van-mat-du-lieu-du-phan-lon-da-chu-dong-sao-luu-du-lieu-105190)