

Tổng quan về bảo mật hệ thống mạng

Bảo mật hệ thống mạng an toàn và hiệu quả sẽ bảo vệ được các thông tin cá nhân của người sử dụng như tài sản, địa chỉ, số điện thoại, cũng như là các thông tin liên quan đến tình hình tài chính, dự án của các tổ chức doanh nghiệp. **Bảo mật** giúp người sử dụng phòng chống lại các hành vi ăn cắp và sử dụng thông tin trái phép nhằm mục đích trục lợi, lừa đảo. Vì thế hãy cùng chúng tôi tìm hiểu chi tiết hơn về vấn đề này nhé.



Khái niệm bảo mật hệ thống mạng

- Bảo mật hệ thống mạng là việc bảo vệ các nguồn dữ liệu, nguồn thông tin trên hệ thống mạng được sử dụng một cách an toàn, tránh được các tác nhân xấu gây ảnh hưởng đến thông tin người dùng trong mạng lưới mạng máy tính.
- Bảo mật hệ thống mạng là việc duy trì tính ổn định của các hoạt động, kiểm tra phương thức vận hành của máy, bảo trì hệ thống thường xuyên để người dùng an tâm khi sử dụng và truy cập vào hệ thống đó.
- Bảo mật mạng sử dụng các công cụ công nghệ để thiết lập nên các phương pháp, thiết lập chương trình và xây dựng một bản phác thảo các

chính sách tối ưu hóa việc bảo mật thông tin, đảm bảo an toàn và điều hành ổn định.

Vai trò của bảo mật hệ thống mạng



- Bảo mật hệ thống mạng giúp doanh nghiệp tránh được các vấn đề rắc rối có thể liên quan đến sự sống còn và tồn tại của mỗi doanh nghiệp đó. Khi các nguồn thông tin về tình hình tài chính, nguồn vốn, nhà đầu tư,... bị tiết lộ sẽ làm ảnh hưởng rất nhiều tới hình ảnh và giá trị của thương hiệu trong tâm trí người tiêu dùng. Hơn thế việc chống lại các vấn đề xâm nhập từ hacker còn giúp doanh nghiệp phát triển ổn định, hoạt động bền vững và lâu dài.

- Hệ thống bảo vệ an toàn thông tin còn vô cùng có ích khi giúp người dùng an tâm hơn khi truy cập, tìm kiếm nguồn dữ liệu trên mạng lưới internet. Họ có thể thoải mái tận hưởng và thỏa sức tra cứu và sử dụng những tiện ích của công nghệ mang lại.

- Hiện trạng tấn công mạng từ các hacker thường xuất hiện phổ biến trong hiện nay. Các hacker sẽ tấn công vào hệ thống mạng dựa trên những lỗ hổng bảo mật, phần mềm độc hại. Việc xâm nhập này sẽ làm cho hệ thống bị tê liệt, không thể vận hành như thế sẽ không thể đáp ứng các tiến trình công việc,
- Bảo mật và an ninh mạng sẽ cung cấp các chính sách và phương án bảo mật hiệu quả, nâng cao hiệu suất làm việc của hệ thống mạng, tối đa hóa năng suất làm việc cho con người.

Phân loại bảo mật hệ thống mạng

Kiểm soát lượng truy cập vào hệ thống



- Việc kiểm soát và phân quyền lượng người truy cập vào hệ thống sẽ hạn chế các mối hiểm nguy đe dọa đến những nguồn cơ sở dữ liệu, gây ra tổn thất rất lớn đối với cá nhân người sử dụng.
- Kiểm soát lượng truy cập sẽ giúp các cá nhân biết được những ai đã truy cập thông tin và ai là người được sử dụng những nguồn thông tin đó.

- Kiểm soát lượng truy cập vào hệ thống sẽ giúp gia tăng tính bảo mật,an toàn của hệ thống thông tin,tăng mức độ khả thi cho việc đảm bảo sự vận hành của hệ thống.

Phần mềm chống virus,mã độc

- Khi người dùng truy cập vào các trang web lạ,phần mềm độc hại các hacker sẽ lợi dụng cơ hội đó để tấn công vào hệ thống mạng máy tính qua các virus,mã độc,...Hacker sẽ dựa vào đó để xâm nhập bất hợp pháp vào mạng lưới thông tin để đánh cắp và tiết lộ thông tin người dùng ra bên ngoài.Vì thế các phần mềm phòng chống virus,mã độc sẽ trở thành một lá chắn vững chãi cho người sử dụng yên tâm khi họ nhập thông tin của mình vào một trang web nào đó.
- Phần mềm chống virus,mã độc ngăn các hành vi xấu xâm nhập vào máy tính,hạn chế quy mô lây lan ra các phần mềm và các thiết bị khác,cũng như là giảm các nguy cơ gây thiệt hại cho hệ thống mạng.

Hệ thống bảo mật



- Bảo mật email cá nhân:email là một phương tiện được dùng nhiều trong đời sống hiện nay.Do đó các hacker sẽ dựa trên đặc điểm này để tấn công vào người sử dụng bằng các hình thức email giả đánh lừa suy nghĩ của người dùng.Một khi người sử dụng truy cập và nhập thông tin cá nhân vào đó thì các thông tin của họ sẽ không còn được bảo vệ nữa.Bảo mật email cá nhân sẽ giúp ngăn chặn các email giả xâm nhập,hạn chế các rủi ro không cần thiết.
- Hệ thống tường lửa:xây dựng hệ thống tường lửa là một yếu tố rất quan trọng trong việc xây dựng hệ thống an ninh mạng.Công dụng của hệ thống này là quản lý nguồn dữ liệu,lưu lượng sao chép và những cá nhân nào sẽ được truy cập vào hệ thống của người sử dụng dựa trên sự phân phó của người sử dụng.
- Hệ thống bảo mật website:bảo mật website đảm bảo các hoạt động được diễn ra an toàn và thuận lợi,tránh được các tác nhân xấu gây hại trên những trang web lạ để người dùng biết và thực hiện các biện pháp ngăn chặn,bảo mật mạng lưới mạng.

Dịch vụ bảo mật hệ thống mạng tại Tú Nguyễn IT

Quy trình thực hiện kiểm tra bảo mật hệ thống mạng

- Thiết lập và kiểm tra tình hình hoạt động của hệ thống.
- Thu thập thông tin từ các nguồn cơ sở dữ liệu,cơ sở hạ tầng,thiết bị máy tính.
- Xây dựng các phương án các kế hoạch phù hợp.
- Thực hiện,giám sát các vấn đề,quá trình đánh giá an toàn hệ thống.
- Đưa ra các nhận xét,đánh giá mức độ khả thi,đo lường hiệu quả tiến trình hoạt động của mạng.
- Có các đề xuất hỗ trợ và nâng cấp,sửa lỗi hệ thống mạng
- Đưa ra các chính sách bảo trì,bảo mật hệ thống mạng.

Dịch vụ giám sát,kiểm tra an toàn hệ thống

- Tăng cường tính an toàn, bảo vệ thông tin hạn chế các rủi ro không đáng có xảy ra đối với bản thân người sử dụng, làm tổn hại đến tinh thần và tài sản của họ khi thông tin bị đưa ra bên ngoài một cách bất hợp pháp.
- Xây dựng các phương án hữu hiệu, nhanh chóng khắc phục các lỗi sai làm ảnh hưởng đến tiến trình làm việc, giảm bớt các chi phí và tiết kiệm thời gian hiệu quả.
- Công dụng của việc sử dụng dịch vụ nâng cấp hệ thống an ninh mạng:
 - o Tiết kiệm thời gian chi phí bảo hành mạng.
 - o Nâng cao năng suất làm việc của hệ thống thúc đẩy hoàn thành tốt nhiệm vụ được giao.
 - o Đảm bảo trạng thái hoạt động của hệ thống luôn ổn định.
 - o Tăng cường bảo mật thông tin mang lại trải nghiệm an toàn cho người sử dụng.

Bài viết trên cung cấp thông tin cơ bản cần biết về vấn đề *bảo mật hệ thống mạng*. Mong rằng qua bài viết này các bạn đọc sẽ tích lũy thêm kiến thức bổ ích cho mình. Mọi thắc mắc xin vui lòng liên hệ với chúng tôi qua HOTLINE **0906953577** để được tư vấn và giải thích chi tiết tại website [Tú Nguyễn IT-Cogihay360](#) và đừng quên theo dõi và đón đọc những bài viết tiếp theo nhé.

Kết nối với Tú Nguyễn IT_Cogihay360

Blogger: <https://www.blogger.com/profile/17555151099530354754>

Blogspot: <https://nguyendotu.blogspot.com/>

Youtube: <https://www.youtube.com/channel/UCkLFVX0G7IHYRDBZdJSR4EQ>

Wordpress: <https://nguyendotu.wordpress.com/>

Gravatar: <https://vi.gravatar.com/nguyendotuit>

Tumblr: <https://nguyendotu.tumblr.com/>

Twitter: <https://twitter.com/nguyendotu>

Diigo: <https://www.diigo.com/profile/nguyendotu>

Evernote: <https://www.evernote.com/secure/ProfileSettings.action>

Getpocket: <https://getpocket.com/@nguyendotu>