CÔNG TY TNHH GIẢI PHÁP VÀ CÔNG NGHỆ SEMTEK

LINUX SECURITY AND HARDENING

Giải pháp bảo mật toàn diện cho website WordPress, bao gồm bảo vệ, củng cố hệ thống Linux và đảm bảo an toàn dữ liệu trước các mối đe dọa tiềm ẩn.

SEMTEK
Results-Driven Business Consulting

(+84) 97-347-8865
sales@semtek.com.vn
Số 2 Lô N đường Lý Chiêu Hoàng, Phường 10, Quận 6, Thành phố Hồ Chí Minh, Việt Nam

CÔNG TY TNHH GIẢI PHÁP VÀ CÔNG NGHỆ SEMTEK
(SEMTEK SOLUTIONS AND TECHNOLOGY CO., LTD.)

VỀ CHÚNG TÔI

Sau 6 năm phát triển, **SEMTEK Solutions** cam kết cách mạng hóa an ninh mạng tại Việt Nam thông qua dịch vụ **"Linux Security and Hardening"** của chúng tôi. Công ty nhằm mục tiêu truyền cảm hứng và hỗ trợ các SMEs nâng cao hiệu suất làm việc bằng cách tận dụng các công cụ bảo mật để tối đa hóa sự bảo vệ hệ thống trên một nền tảng duy nhất.

Dịch vụ **"Linux Security and Hardening"** của **SEMTEK** hỗ trợ các quản trị viên bảo mật hệ thống, tăng cường độ an toàn và quản lý các nguy cơ một cách hiệu quả. Không chỉ đơn thuần là cung cấp giải pháp, **SEMTEK Solutions** mang đến các sáng kiến bảo mật giúp các **SMEs** cải thiện khả năng phòng thủ của hệ thống. Với nền tảng công nghệ mạnh mẽ và quy trình bảo mật chuẩn hóa được tích lũy qua 6 năm, **SEMTEK Solutions** giúp các doanh nghiệp củng cố hệ thống của mình một cách hiệu quả.

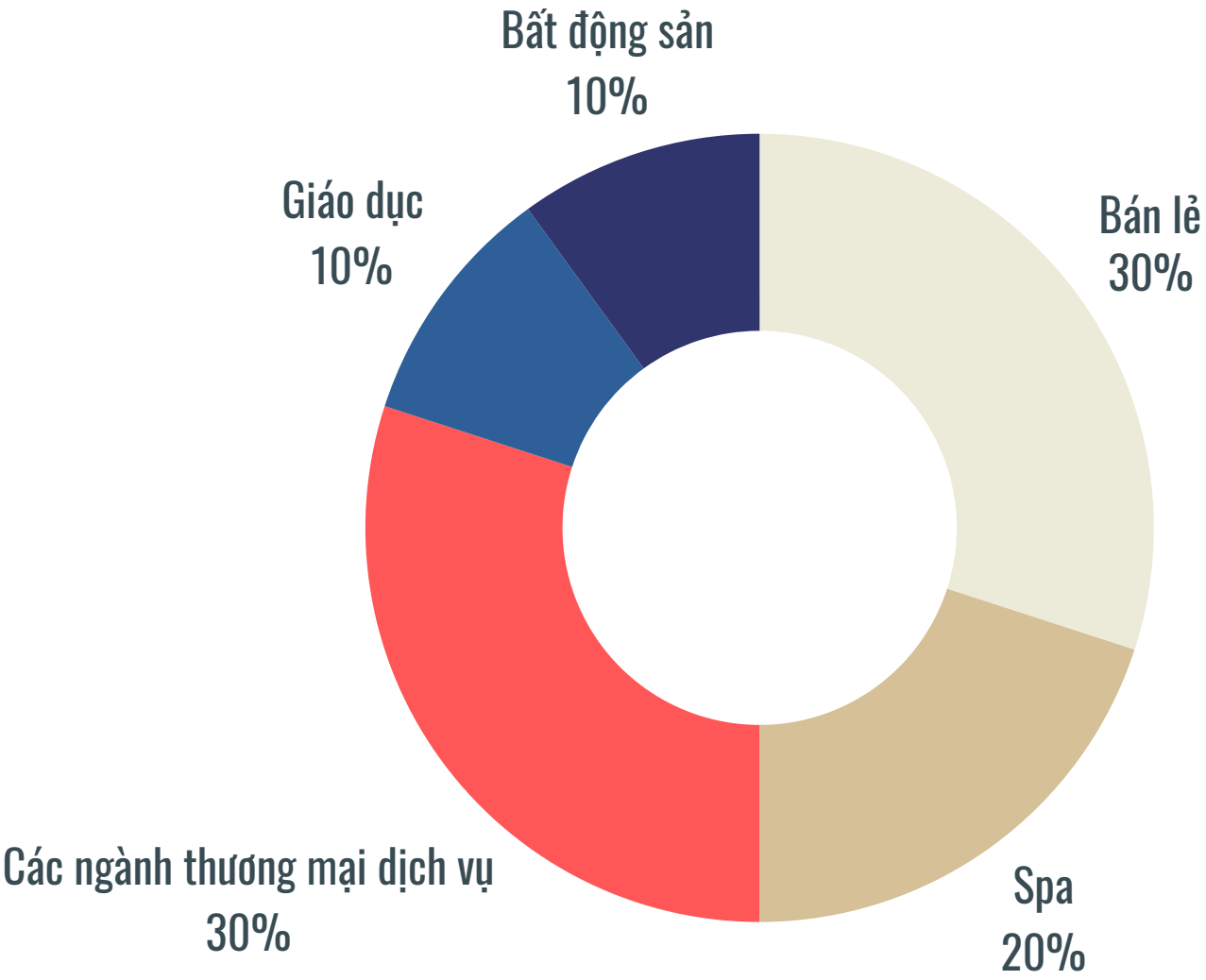
KHÁCH HÀNG MỤC TIÊU CỦA CHÚNG TÔI

Bằng cách tập trung vào các nhóm khách hàng này, chúng tôi mong muốn mang đến những giải pháp tối ưu phù hợp, giúp họ cải thiện hiệu quả quản lý và phát triển bền vững hơn.

Quy mô: Các doanh nghiệp vừa và nhỏ (SMEs)
Vai trò trong tổ chức:

- Người sáng lập
- Các giám đốc cấp cao
- Các nhà quản lý trong lĩnh vực bán hàng, marketing và dịch vụ khách hàng

CÁC NGÀNH NGHỀ CHÍNH CỦA KHÁCH HÀNG



LINUX SECURITY AND HARDENING

BẢO MẬT HỆ THỐNG, TĂNG CƯỜNG ĐỘ AN TOÀN & QUẢN LÝ CÁC NGUY CƠ

Dịch vụ **Linux Security and Hardening** của **SEMTEK** hỗ trợ các quản trị viên bảo mật hệ thống, tăng cường độ an toàn và quản lý các nguy cơ một cách hiệu quả. Không chỉ đơn thuần là cung cấp giải pháp, **SEMTEK Solutions** mang đến các sáng kiến bảo mật giúp các **SMEs** cải thiện khả năng phòng thủ của hệ thống. Với nền tảng công nghệ mạnh mẽ và quy trình bảo mật chuẩn hóa được tích lũy qua 6 năm, **SEMTEK Solutions** giúp các doanh nghiệp củng cố hệ thống của mình một cách hiệu quả.

NHỮNG KHÓ KHĂN DOANH NGHIỆP GẶP PHẢI TRONG QUẢN LÝ VẬN HÀNH

- **Đối phó với các mối đe dọa mạng**: Nhiều doanh nghiệp nhỏ gặp khó khăn trong việc bảo vệ hệ thống Linux khỏi truy cập trái phép và các cuộc tấn công mạng do thiếu nguồn lực và chuyên môn.
- **Bảo mật trước truy cập vật lý:** Việc đảm bảo an toàn hệ thống ngay cả khi kẻ tấn công có quyền truy cập vật lý là thách thức do hạn chế về cơ sở hạ tầng bảo mật.
- **Chính sách mật khẩu và tài khoản không đủ mạnh**: Các doanh nghiệp SMEs thường thiếu các chính sách mật khẩu mạnh mẽ và quản lý thời hạn tài khoản hiệu quả, dẫn đến nguy cơ an ninh.
- **Thiếu nâng cao bảo mật SSH**: Nhiều doanh nghiệp nhỏ không áp dụng các thực hành tốt nhất để bảo vệ cấu hình ssh, dẫn đến nguy cơ truy cập trái phép.
- **Chiến lược phòng thủ mạng yếu**: Khả năng tăng cường bảo mật mạng để giảm thiểu các lỗ hổng thường bị hạn chế do thiếu nhân lực chuyên môn.
- **Khó khăn trong quản lý cổng và dịch vụ**: Khả năng quét cổng và phát hiện dịch vụ mạng để xác định điểm xâm nhập tiềm năng thường bị hạn chế.
- **Cấu hình tường lửa Linux phức tạp**:
Nhiều SMEs gặp khó khăn trong việc hiểu và cấu hình tường lửa linux để bảo vệ hạ tầng.
- **Rủi ro bảo vệ tài khoản "root"**: Bảo mật tài khoản siêu người dùng khỏi sự lạm dụng hoặc xâm phạm là thách thức lớn.
- **Chia sẻ tài khoản không an toàn**: Việc đảm bảo chia sẻ tài khoản an toàn và có kiểm tra trách nhiệm không được thực thi đầy đủ.
- **Thiếu bảo mật hệ thống tập tin và mã hóa**: Các giao thức bảo mật và mã hóa dữ liệu nhạy cảm chưa được triển khai hiệu quả.
- **Quản lý quyền truy cập còn hạn chế:**
Khó khăn trong việc sử dụng các chế độ đặc biệt, thuộc tính tập tin và acls để kiểm soát truy cập chi tiết.
- **Sao lưu và phục hồi dữ liệu cho các website lớn một cách tự động:**
Thiết lập các lịch trình sao lưu định kỳ (hàng ngày, hàng tuần hoặc hàng tháng) để đảm bảo rằng tất cả dữ liệu được sao lưu một cách hệ thống và không bị mất mát.

GIẢI PHÁP "LINUX SECURITY AND HARDENING" ĐƯỢC THỰC HIỆN GỒM

1. **Cài đặt máy chủ website:**
Cấu hình máy chủ với LAMP (Linux, Apache, MySQL, PHP) trên Ubuntu, hỗ trợ lưu trữ các trang web WordPress và ứng dụng web PHP.

2. **Bảo mật tập tin nâng cao:**
Cấu hình mã hóa dữ liệu, hạn chế quyền truy cập tập tin và áp dụng các chính sách bảo mật nghiêm ngặt để bảo vệ hệ thống tệp.

3. **Cài đặt phần mềm diệt virus:**
Triển khai và cấu hình ClamAV để bảo vệ máy chủ khỏi các phần mềm độc hại và virus.

4. **Tối ưu hóa bộ nhớ:**
Tạo hoặc mở rộng các tập tin swap, đảm bảo hiệu suất máy chủ ổn định ngay cả khi tải nặng.

5. **Cấu hình tường lửa (Firewall):**
Thiết lập và quản lý tường lửa (Firewall) như UFW hoặc iptables để bảo vệ chống truy cập trái phép và chặn các kết nối nguy hiểm.

6. **Bảo mật cơ sở dữ liệu:**
Cài đặt và bảo mật phpMyAdmin, bao gồm các biện pháp bảo vệ truy cập và bảo mật cơ sở dữ liệu MySQL.

7. **Thay đổi cổng SSH mặc định:**
Thay đổi cổng SSH mặc định để tăng cường bảo mật, ngăn chặn các cuộc tấn công brute force.

8. **Cập nhật và cấu hình php:**
Đảm bảo máy chủ luôn chạy phiên bản PHP mới nhất, tối ưu hóa cấu hình để tăng cường hiệu suất và bảo mật.

9. **Quản lý nhiệm vụ định kỳ:**
Thiết lập cron job để tự động hóa các công việc như sao lưu, dọn dẹp file log, hoặc kiểm tra hệ thống.

10. **Giải pháp sao lưu tự động:**
Phát triển các script shell cho việc sao lưu tự động, bảo vệ dữ liệu theo lịch trình hàng ngày, hàng tuần hoặc hàng tháng.

GIẢI PHÁP "LINUX SECURITY AND HARDENING" LÀ GÌ?

Dịch vụ **"Linux Security and Hardening"** cung cấp một loạt các giải pháp bảo mật mạnh mẽ và các thực hành tối ưu hóa máy chủ. Điều này bao gồm các biện pháp bảo vệ chống lại các cuộc tấn công mạng, bảo mật truy cập vật lý cho máy chủ, phát triển và triển khai chính sách mật khẩu vững chắc, cũng như củng cố giao thức SSH để phòng ngừa truy cập trái phép.

KHI NÀO NÊN SỬ DỤNG GIẢI PHÁP "LINUX SECURITY AND HARDENING"?

When?

Dịch vụ **"Linux Security and Hardening"** nên được thực hiện trong suốt vòng đời của hệ thống, từ giai đoạn thiết lập ban đầu đến bảo trì định kỳ. Cập nhật bảo mật thường xuyên và sao lưu tự động được thiết lập để duy trì bảo vệ không ngừng và phục hồi nhanh chóng khi xảy ra sự cố. Điều này đảm bảo rằng hệ thống luôn ở trạng thái bảo vệ tốt nhất và có thể ứng phó kịp thời với các mối đe dọa mới.

TẠI SAO CẦN SỬ DỤNG GIẢI PHÁP "LINUX SECURITY AND HARDENING"?

Sử dụng dịch vụ "**Linux Security and Hardening**" nhằm bảo vệ dữ liệu quan trọng khỏi các mối đe dọa bảo mật ngày càng tinh vi, ngăn chặn sự truy cập trái phép và đảm bảo tính liên tục cho hoạt động kinh doanh. Bằng cách tối ưu hóa và bảo mật hệ thống, doanh nghiệp có thể duy trì hiệu suất hoạt động cao, giảm thiểu rủi ro và chi phí liên quan đến sự cố bảo mật.

Why?

AI NÊN SỬ DỤNG GIẢI PHÁP "LINUX SECURITY AND HARDENING"

Who?

Dịch vụ "**Linux Security and Hardening**" hướng tới các doanh nghiệp và tổ chức sử dụng hệ thống máy chủ Linux. Đặc biệt, nó dành cho các công ty lưu trữ website WordPress hoặc các ứng dụng web dựa trên PHP, nơi mà tính bảo mật và hiệu suất của hệ thống là yếu tố then chốt cho hoạt động kinh doanh.

SỬ DỤNG GIẢI PHÁP "LINUX SECURITY AND HARDENING" Ở ĐÂU?

Dịch vụ **"Linux Security and Hardening"** áp dụng trên hệ thống cơ sở hạ tầng máy chủ Linux của doanh nghiệp. Nó có thể được triển khai trên các máy chủ vật lý tại chỗ hoặc trên các nền tảng đám mây, giúp linh hoạt đáp ứng nhu cầu riêng của mỗi doanh nghiệp. Việc triển khai dịch vụ có thể mở rộng đến hệ thống tập tin và cấu hình bảo mật mạng trên toàn bộ hệ thống.

Where?

6 LỢI ÍCH CỦA GIẢI PHÁP "LINUX SECURITY AND HARDENING" MANG LẠI CHO DOANH NGHIỆP SMES?

↓90%

Bảo vệ chống lại các mối đe dọa mạng:
Doanh nghiệp giảm thiểu rủi ro bị tấn công từ hacker và phần mềm độc hại. Các nghiên cứu cho thấy có đến 60% các SME không có các biện pháp bảo vệ đầy đủ gặp phải tấn công mạng trong năm đầu tiên. Tuy nhiên, doanh nghiệp áp dụng giải pháp bảo mật toàn diện có thể giảm tới 90% rủi ro bị xâm nhập trái phép.

↓5%

Bảo mật trước truy cập vật lý:
Bảo vệ hệ thống ngay cả khi kẻ tấn công có quyền truy cập vật lý, giảm nguy cơ bị đánh cắp dữ liệu. Trong một khảo sát, 30% các vi phạm an ninh xuất phát từ việc không bảo vệ tốt truy cập vật lý. Việc triển khai các biện pháp bảo mật vật lý đã giúp giảm lỗ hổng này xuống còn 5%.

↓70%

Chính sách mật khẩu và tài khoản mạnh mẽ:
Tăng cường an ninh hệ thống qua việc quản lý mật khẩu và tài khoản, ngăn chặn truy cập trái phép. Công ty áp dụng chính sách mật khẩu nghiêm ngặt đã giảm 70% các vụ việc truy cập trái phép so với những công ty không áp dụng.

↓80%

Ngăn chặn truy cập trái phép qua cổng SSH:
Ngăn chặn truy cập trái phép qua cổng SSH bằng cách củng cố cấu hình bảo mật. Theo các chuyên gia, bảo mật SSH giúp giảm đến 80% các nguy cơ bị xâm nhập thông qua giao thức SSH.

↓50%

Tăng cường phòng thủ mạng:
Nâng cao khả năng phát hiện và ngăn chặn các lỗ hổng mạng, bảo vệ hệ thống khỏi các cuộc tấn công tinh vi. Doanh nghiệp áp dụng chiến thuật phòng thủ nâng cao có thể giảm 50% các rủi ro về bảo mật mạng theo thống kê từ các nhà cung cấp dịch vụ bảo mật hàng đầu.

↓60%

Quản lý cổng và dịch vụ hiệu quả:
Xác định và quản lý các điểm truy cập tiềm năng để bảo vệ doanh nghiệp khỏi rủi ro an ninh. Việc thực hiện quét cổng và quản lý dịch vụ đã giúp giảm tới 60% khả năng bị xâm nhập qua các điểm yếu dịch vụ không được bảo mật.

CÔNG TY TNHH GIẢI PHÁP VÀ CÔNG NGHỆ SEMTEK

(SEMTEK SOLUTIONS AND TECHNOLOGY CO., LTD.)

Nurturing Global Thinkers, Shaping Scientific Leaders

Thông tin liên hệ

2N, Lý Chiêu Hoàng, Phường 10, Quận 6, T.P HCM

(+84) 97-347-8865 | (+84) 98-300-9285

sales@semtek.com.vn

www.semtek.com.vn

SEMTEK

Results-Driven Business Consulting