KONICA MINOLTA

How businesses adapt to stay operational in the virtual environment

Giải pháp nào cho doanh nghiệp duy trì hoạt động trong "môi trường ảo"?

In the age of digital transformation, cybercrime has emerged as today's fastest-growing form of criminal activity, with 43% of online attacks now aimed at the Small Medium-sized Enterprises (SME)s, yet only 14% are prepared to defend themselves.[1] What this means to business owners, is the increasing need to be more cybersecurity conscious and to invest more to defend themselves against cyberattacks that pose significant threat to their IT infrastructure. Companies need to educate their staff to send any suspicious targeted social engineering attack such as scareware directly to cybersecurity team for analysis, and business owners also needs to work closely with international law enforcement agencies as well as national regulatory bodies to build a comprehensive cyber defense.

Hoạt động của tội phạm công nghệ cao diễn ra ngày càng phức tạp, nhất là trong thời kì phát triển mạnh mẽ của chuyển đổi kỹ thuật số, với hơn 43% cuộc tấn công trực tuyến nhằm vào các doanh nghiệp vừa và nhỏ (SME), nhưng chỉ có 14% trong số đó được xây dựng hệ thống bảo vệ những rủi ro tấn công từ mạng lưới này. [1] Vậy, điều này có ý nghĩa gì đối với chủ doanh nghiệp? Ý thức về an ninh mạng và nhu cầu đầu tư nhiều hơn vào cơ sở hạ tầng thông tin đang được các doanh nghiệp quan tâm để chủ động bảo vệ mình trước các mối đe dọa do tấn công mạng gây ra. Mỗi nhân viên cần được lưu ý về việc thông báo ngay cho đội ngũ công nghệ thông tin (CNTT) khi phát hiện có bất cứ cuộc tấn công mạng có mục tiêu đáng ngờ cho hệ thống bảo mật của doanh nghiệp để họ điều tra và phân tích. Đồng thời, chủ doanh nghiệp cũng cần hợp tác chặt chẽ với các cơ quan thực thi pháp luật quốc tế và quốc gia sở tại để xây dựng hệ thống bảo vệ không gian mạng toàn diện.

As COVID-19 pandemic continues to sweep the globe, cybercriminals around the world undoubtedly are poised to capitalize on the crisis by launching a different kind of "virus". Companies should ensure all corporate owned or managed devices are equipped with essential security capabilities and adhere to security best practices in remote environments. These critical capabilities such as the ability to:[2]

Khi đại dịch COVID-19 vẫn đang lan rộng trên toàn cầu, cũng là thời cơ thích hợp để tội phạm công nghệ cao tận dụng cuộc khủng hoảng và tạo ra một loại "virus" khác. Các doanh nghiệp cần đảm bảo tất cả các thiết bị thuộc sở hữu hoặc quản lý của công ty đều được trang bị chức năng bảo mật thiết yếu và tuân thủ các bài học thực tế về hệ thống bảo mật từ xa. Một số chức năng quan trọng: [2]

Konica Minolta Business Solutions Vietnam Co., Ltd.
Head Office: Unit 3, 8th Fl., Bitexco Financial Tower, No. 2 Hai Trieu St., Dist. 1, HCMC, Vietnam | **Tel:** +84 (28) 3915 4242 | **Fax:** +84 (28) 3915 3670
Branch Office: 05 Nguyen Ngoc Vu St., Cau Giay Dist., Hanoi, Vietnam | **Tel:** +84 (24) 3776 7023 | **Fax:** +84 (24) 3776 7025
Email: info.bvn@konicaminolta.com | **Website:** www.konicaminolta.com/vn-vi/ | **Facebook:** Konica Minolta Vietnam

- Securely connect users to their business-critical cloud and on-premise applications, such as video teleconferencing applications which are increasingly relevant for remote work environments
  Kết nối an toàn người dùng với ứng dụng điện toán đám mây và ứng dụng có sẵn. Một ví dụ điển hình được sử dụng phổ biến trong môi trường làm việc từ xa hiện nay là hội nghị video trực tuyến.

- Provide endpoint protection on all laptops and mobile devices, including VPN tools with encryption
  Cung cấp giải pháp bảo vệ điểm cuối trên tất cả máy tính xách tay và thiết bị di động, các công cụ VPN có mã hóa

- Enforce multi-factor authentication (MFA)
  Triển khai xác thực đa nhân tố (MFA)
- Block exploits, malware and command-and-control (C2) traffic using real-time, automated threat intelligence
  Ngăn chặn các phần mềm độc hại, kiểm soát lưu lượng truy cập theo thời gian thực, cảnh báo tự động các mối đe dọa có thể xảy ra.

- Filter malicious domain URLs and perform DNS sinkholing to thwart common phishing attacks
  Lọc các miền URL độc hại và thực hiện cơ chế DNS để ngăn chặn và kiểm soát các cuộc tấn công từ tội phạm công nghệ cao.

While organizations may eventually face the prospect of functioning with little to no personnel on-site and other important support functions, and businesses are trying to figure out how to stay operational in a virtual world, the need to invest in cybersecurity solutions to protect their businesses, especially since the loss of personal information and impact of a cyber-attack can be far greater than the cost of getting protected in the first place.[3]

Với sự chuyển đổi hình thức hoạt động của nền kinh tế, doanh nghiệp sẽ phải dần thích ứng và đối mặt với vấn đề hoạt động trong sự hạn chế về nhân công và một số chức năng hỗ trợ khác. Họ đang cố gắng tìm ra giải pháp để duy trì hoạt động trong một "môi trường ảo" bằng cách đầu tư vào các giải pháp an ninh mạng để bảo vệ doanh nghiệp của mình. Bài toán về chi phí được đặt ra khi thiệt hại do rò rỉ thông tin cá nhân và hệ quả của cuộc tấn công mạng có thể lớn hơn nhiều so với chi phí ban đầu doanh nghiệp bỏ ra để xây dựng hệ thống an ninh mạng.[3]

Hacking techniques are constantly evolving and is increasingly getting more complex. As a result, cybersecurity is a growing concern for the organization globally. Legacy technologies such as firewall and antivirus software are proving inadequate in this evolving cyber threat landscape. Vulnerabilities in the computer system security have been exploited by unethical hackers, resulting in millions of personal information being stolen, sold or held for ransom, creating a debilitating impact on the economy. With Konica Minolta CyberSecure Platform, we provide multi-featured defense in a box which helps organizations to mitigate cyber threats instantly.[4]

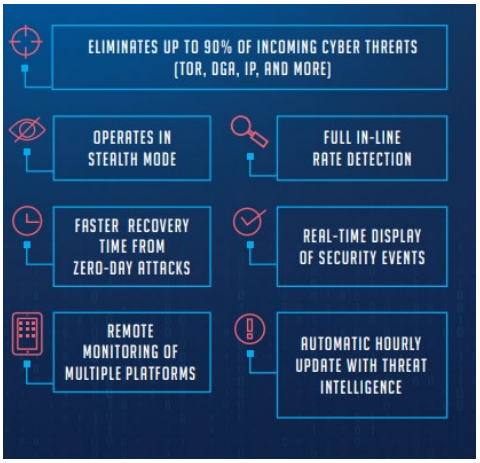
Các kỹ thuật hack (hành động thâm nhập mang tính phá hoại) liên tục phát triển và ngày càng phức tạp hơn. Do đó, an ninh mạng là mối quan tâm lớn của mọi tổ chức trên toàn cầu. Các công nghệ cũ như tường lửa và phần mềm chống vi-rút đang không còn đầy đủ khả năng chống lại những mối đe dọa từ an ninh mạng trong bối cảnh phát triển như hiện nay. Các lỗ hổng trong bảo mật hệ thống máy tính đã bị các tội phạm công nghệ khai thác, dẫn đến hàng triệu thông tin cá nhân bị đánh cắp, bán hoặc giữ để đòi tiền chuộc, tạo ra tác động làm suy yếu nền kinh tế. Với Nền tảng

CyberSecure của Konica Minolta, chúng tôi cung cấp gói giải pháp cho hệ thống phòng thủ đa tính năng giúp các tổ chức giảm thiểu các mối đe dọa từ an ninh mạng ngay lập tức.[4]

An innovative and automated way of securing your network, the CyberSecure Platform typically deploys in-line, where the packet is processed in lightning speed with comprehensive security engine that prevents intrusion. Most importantly, the CyberSecure Platform is invisible to the hackers, thus provides a robust protection to your network.

Nền tảng CyberSecure được triển khai nội tuyến, trong đó gói giải pháp được xử lý với tốc độ cực nhanh bằng công cụ bảo mật toàn diện giúp ngăn chặn sự xâm nhập từ bên ngoài, đảm bảo an toàn cho hệ thống mạng của doanh nghiệp một cách sáng tạo và tự động. Điểm quan trọng đặc biệt là tội phạm công nghệ không thể nào phát hiện được sự tồn tại của Nền tảng CyberSecure trong hệ thống, do đó nền tảng này mang đến sự bảo vệ mạnh mẽ cho mạng lưới an ninh của doanh nghiệp.

Key Features
Chức năng



Key Benefits of CyberSecure Platform
Lợi ích chính của Nền tảng CyberSecure

- Invisible to cyber criminals (Stealth mode)
  Vô hình với tội phạm công nghệ (Chế độ tàng hình)
- Malicious packets are dropped even before it reaches the firewall (bi-directional)
  Các phầm mềm độc hại bị vô hiệu hóa ngay trước khi nó tấn công tường lửa (hai chiều)
- Deep Packet Inspection (DPI)
  Phân tích sâu các gói (DPI)

To find out more about CyberSecure Platform
Visit: https://www.konicaminolta.sg/business/solutions/cybersecure-platform/

Để tìm hiểu thêm thông tin về Nền tảng CyberSecure, vui lòng truy cập đường dẫn bên dưới
https://www.konicaminolta.sg/business/solutions/cybersecure-platform/

[1].https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html
[2]. https://www.weforum.org/agenda/2020/03/covid-19-cyberattacks-working-from-home/

[3].https://www.straitstimes.com/world/united-states/coronavirus-themed-cyberattacks-surge-as-more-employees-forced-to-work-from-home
[4].https://www.konicaminolta.sg/business/solutions/cybersecure-platform/