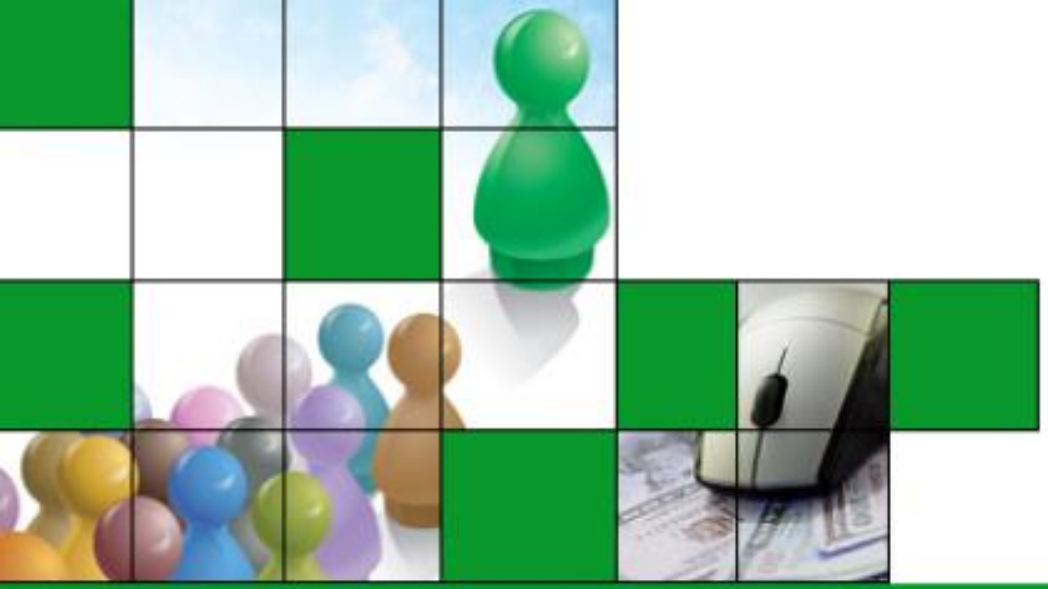


Đổi mới & nâng cấp hệ thống an ninh thông tin trong thanh toán:

Đảm bảo an toàn cho các giao dịch trực tuyến

Nội dung

- Nguy cơ an toàn thông tin
- Hệ thống bảo mật
- Công nghệ
- Nhân sự
- Quy trình

Nguy cơ an toàn thông tin

- Tội phạm tin học trong nước và trên thế giới ngày càng gia tăng
- Các phương pháp tấn công đa dạng:
  - Khai thác lỗ hổng bảo mật phổ biến: Injection, XSS, XSRF…
  - Sử dụng Virus, Trojan, Malware…
  - Phishing
  - Tấn công MITM, MITB
  - Tấn công từ chối dịch vụ (DoS, DDoS)

Một số vụ tấn công vào ngân hàng gần đây

- Kaspersky Security Bulletin 2015: gần 2 triệu máy tính nhiễm malware lấy trộm tiền từ tài khoản ngân hàng
- 2/2015: Nhóm hacker “Carbanak” tấn công 100 ngân hàng trên 30 quốc gia, đánh cắp 1 tỷ đô la Mỹ.
- 10/2015: Hacker dùng virus đánh cắp 20 triệu bảng từ nhiều tài khoản ngân hàng tại Anh.
- 1/2016: Hacker sử dụng DDoS đánh sập hệ thống ngân hàng trực tuyến của HSBC vào ngày trả lương cuối tháng.

Một số vụ tấn công vào ngân hàng gần đây

EXPRESS

Is YOUR compu

Hackers use viru

MILLION from

accounts

CYBER criminals have stolen £20 MILLION

sophisticated computer malware, investigat

By NICK GUTTERIDGE

PUBLISHED: 20:50, Tue, Oct 13, 2015 | UPDATED: 12:53, Mon, Oct 19, 2015

SHARE TWEET 15

Forbes / Security

The Little Black Book of

JAN 29, 2016 @ 08:11 AM 2,012 VIEWS

HSBC Calls In Cops To Chase DDoS Attackers Who Took Online Banking Down

Thomas Fox-Brewster, FORBES STAFF

I cover crime, privacy and security in digital and physical forms.

FOLLOW ON FORBES (173)

FULL BIO

HSBC said today it was working with local police to find those who disrupted its online banking services with a denial of service attack, as customers complained of not being able to access their accounts. The attack was made even more painful for customers as the last Friday of the month is a traditional payday in the UK, the home of HSBC.

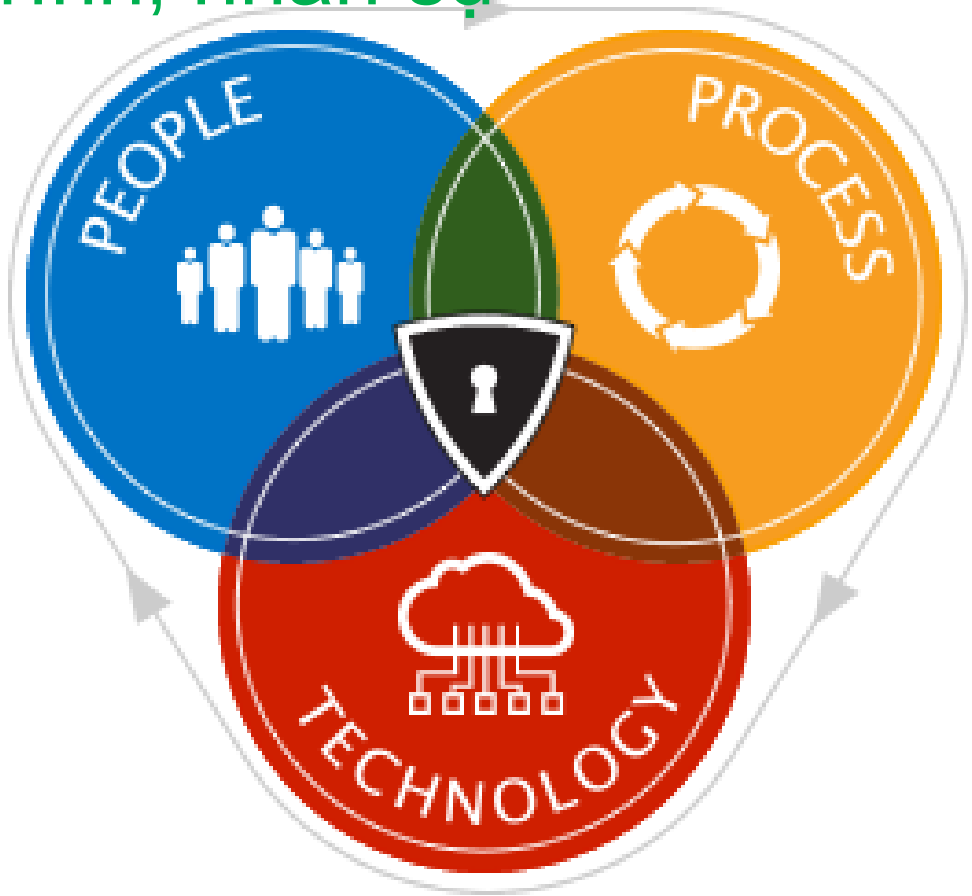
Training & Certification Incident Response

Hackers Hit 100 Banks in 'Unprecedented' $1 Billion Cyber Heist: Kaspersky Lab

By Mike Lennon on February 15, 2015

Hệ thống bảo mật

- Kết hợp của 3 thành phần: công nghệ, quy trình, nhân sự

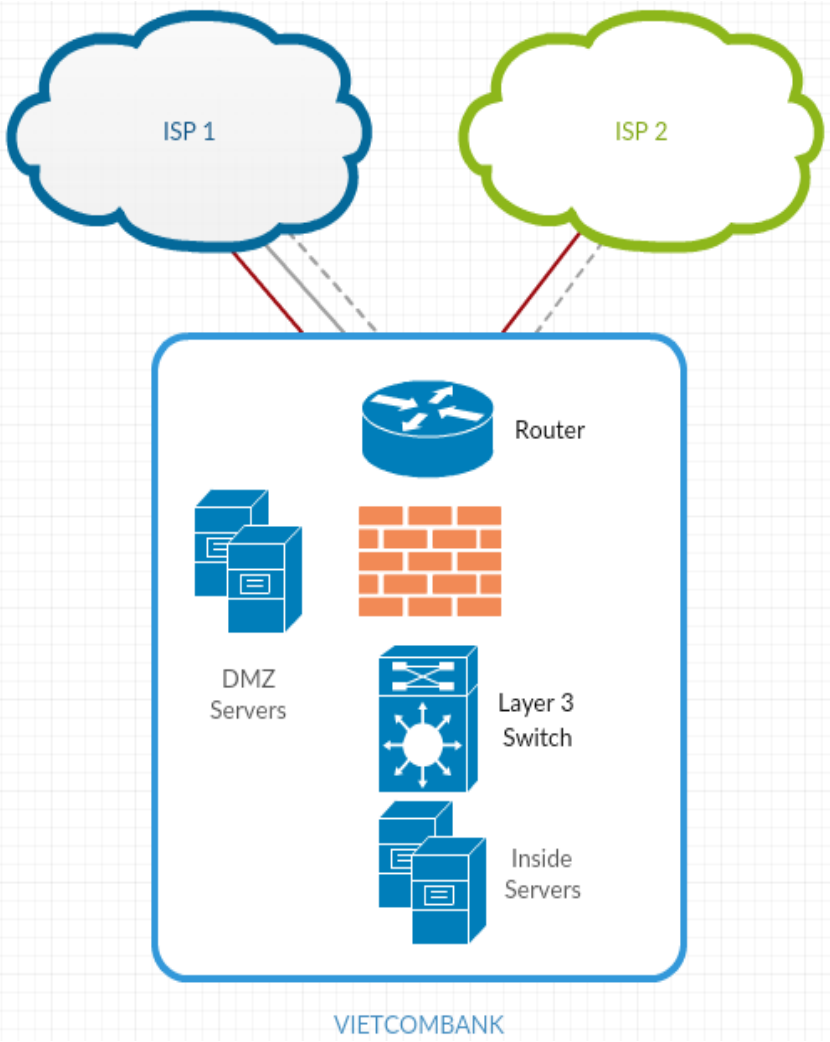


Kiến trúc bảo mật mạng

- Mô hình mạng 3-tier đáp ứng theo yêu cầu ứng dụng Internet Banking
- Các giải pháp đa dạng nhằm nâng cao tính bảo mật trên toàn hệ thống: WAF, Firewall, IPS, phòng chống APT, phòng chống DDoS...

Kết nối đến các nhà cung cấp dịch vụ Internet

- 2 nhà cung cấp dịch vụ. Mỗi nhà cung cấp có nhiều đường vật lý.
- Băng thông cao để đề phòng tấn công DDoS làm đầy lưu lượng.
- Lọc dữ liệu ngay từ router đầu vào: No discovery protocols, đặt access-control list.



Bảo mật ứng dụng

- Hệ thống ngân hàng điện tử được xây dựng với tiêu chí bảo mật được đặt lên hàng đầu.
- Chống các tấn công phổ biến:
  - Injection (SQL, Xpath, LDAP…)
  - Cross-site Scripting (XSS)
  - Cross-site Request Forgery (XSRF)
  - Brute-Force

Mã hóa dữ liệu

- Các dữ liệu nhạy cảm được mã hóa bằng các thuật toán mã hóa bảo mật nhất:
  - Symmetric: AES, Camellia, ARIA, SEED…
  - Asymmetric: RSA, DSA, D-H, KCDSA…
  - Hash: SHA-1, SHA-2 (224-512)…
- Sử dụng HSM cho việc sinh khóa, lưu trữ khóa, mã hóa, giải mã
- Thuật toán mã hóa được định kỳ rà soát và nâng cấp

Kiểm tra bảo mật

- Thường xuyên kiểm tra hệ thống bằng công cụ kiểm tra lỗ hổng bảo mật

acunetix

AppScan

IBM Security

Trustwave®

N-Stalker®
THE WEB SECURITY SPECIALISTS

Nessus®
vulnerability scanner

Xác thực đa nhân tố

- Sử dụng xác thực đa nhân tố để tăng cường bảo mật cho các giao dịch trực tuyến

1

What you know
(Cái bạn biết)

2

What you have
(Cái bạn có)

3

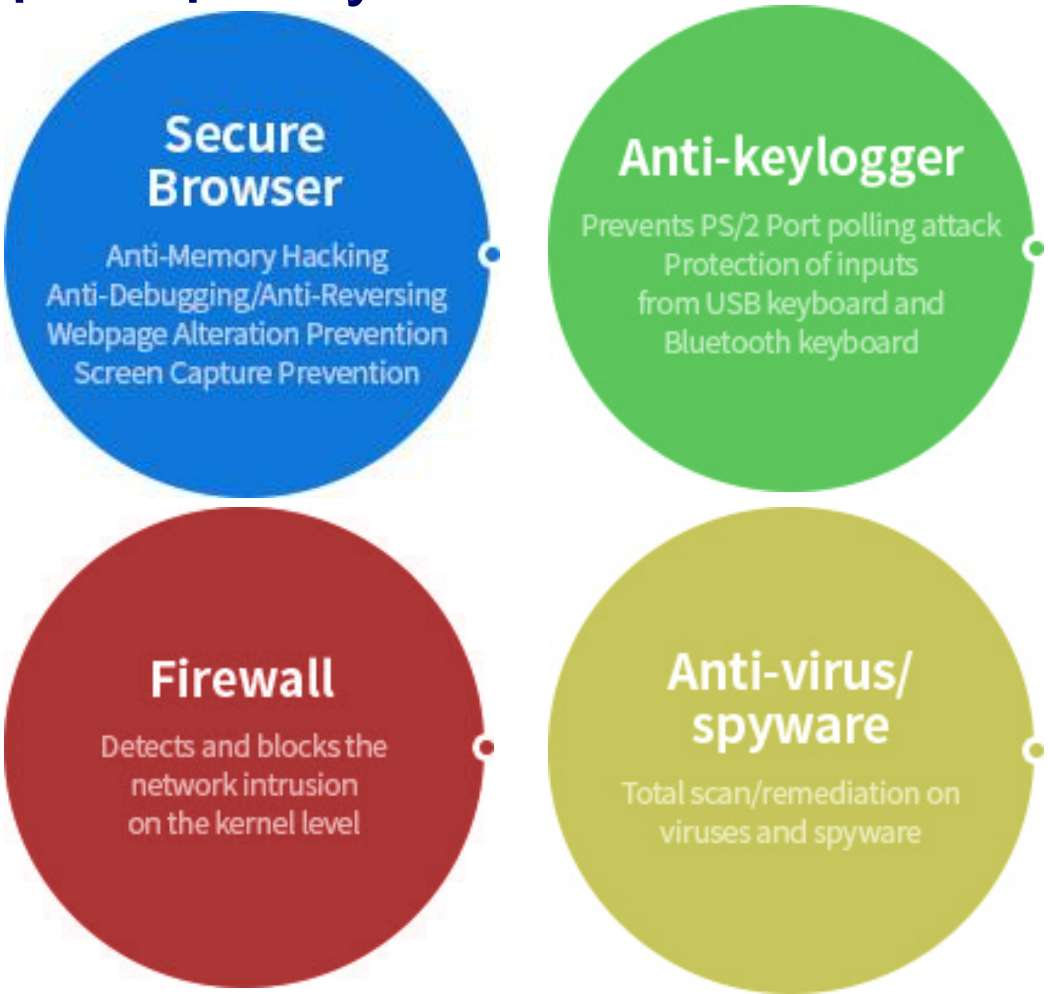
What you are
(Cái chính là bạn)

One-Time Password (OTP)

- Các hình thức OTP phổ biến:
  - Tin nhắn SMS
  - Token bấm số
  - Thẻ EMV
  - Matrix
  - PKI token
  - Mobile app

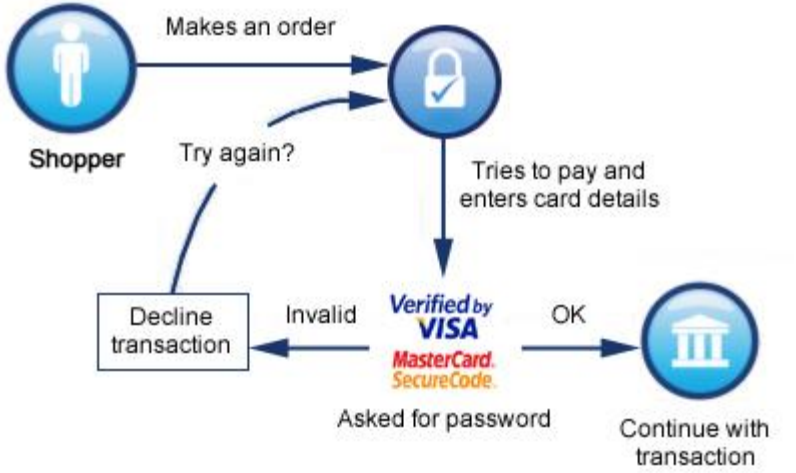
Bảo mật phía khách hàng

- Giải pháp bảo vệ khách hàng khi thực hiện các giao dịch trực tuyến



3-D Secure

- Cơ chế bảo mật của Visa/ Mastercard/ JCB/ Amex cho các giao dịch thanh toán bằng thẻ tín dụng/ ghi nợ



Verified by VISA · American Express SafeKey · MasterCard SecureCode · JCB J/Secure

Hệ thống giám sát, cảnh báo

- Thường xuyên theo dõi, giám sát hoạt động của hệ thống
- Tự động phát hiện và cảnh báo các cuộc tấn công vào hệ thống
- Phát hiện các truy cập trái phép

Chống giả mạo giao dịch

- Hệ thống tự động theo dõi, phân tích các giao dịch trực tuyến
- Phát hiện các giao dịch bất thường, giả mạo

Nhân sự

- Đội ngũ nhân sự chuyên trách
- Liên tục cập nhật các kiến thức về bảo mật
- Được đào tạo chuyên nghiệp, đạt các chứng chỉ về bảo mật

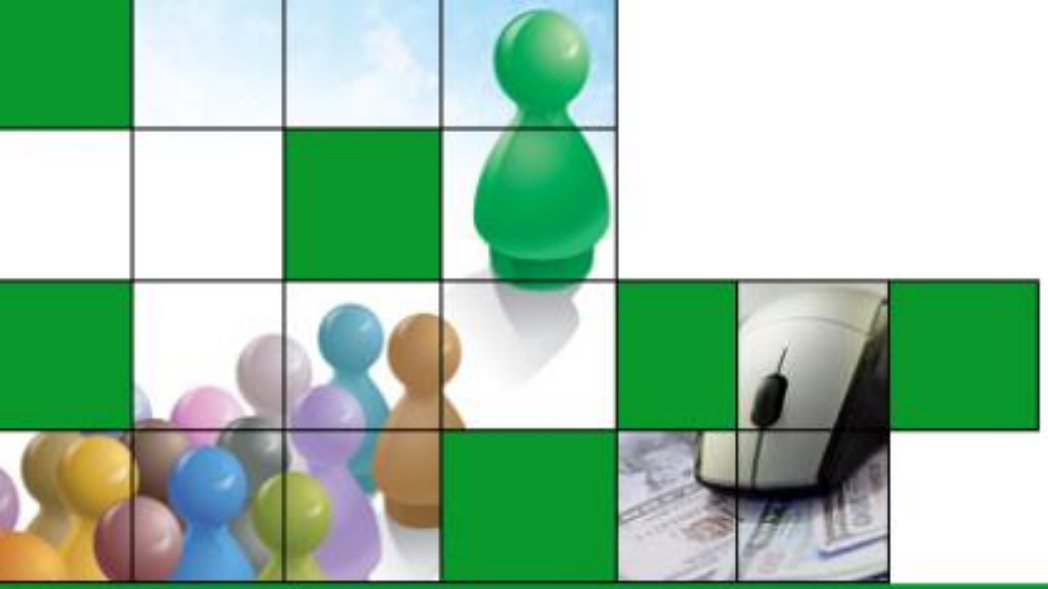
Chính sách, quy trình

- Xây dựng đầy đủ các chính sách, quy trình bảo mật cho hệ thống CNTT nói chung và hệ thống ngân hàng điện tử nói riêng
  - Quản lý tài sản CNTT
  - Quản lý nhân sự CNTT
  - Kiểm soát truy cập hệ thống CNTT
  - Quy định về mã hóa
  - An toàn môi trường hoạt động
  - Vận hành và bảo trì hệ thống CNTT
  - Nâng cấp phần mềm ứng dụng
  - Quản lý sự thay đổi
  - Quản lý sự cố CNTT
  - Duy trì tính liên tục của hoạt động kinh doanh

- Định kỳ rà soát, cập nhật chính sách, quy trình

Tiêu chuẩn bảo mật

- Tuân thủ thông tư 29/2011/TT-NHNN của NHNN về ngân hàng điện tử và nghị định 52/2013/NĐ-CP của chính phủ về thương mại điện tử
- Đáp ứng các chuẩn bảo mật quốc tế: ISO/IEC 27001, PCI DSS



Vietcombank
Chung niềm tin vững tương lai

Thank You !