Ethics in Information Technology, Fourth Edition

Chapter 3
Computer and Internet Crime

George W. Reynolds

Lecturer : Mansour Rousta Zadeh

1

اصول اخلاقی در فناوری اطلاعات – ویرایش چهارم (جورج دبلیو رینالدز)

- درس اخلاق حرفه‌ای در فناوری اطلاعات
  - مدرس : منصور روستازاده
- فصل سوم ، گفتار سوم
  - جرایم کامپیوتری و اینترنتی
- هفته نهم
  - نیمسال دوم ۹۲-۹۳

SMS : ۰۹۳۹ – ۱۰۱ ۰۰۲۴

eMail : EIT @ EXIST . IR

Establishing a Security Policy

- A security policy defines:
  - Organization's security requirements
  - Controls and sanctions needed to meet the requirements
- Delineates responsibilities and expected behavior
- Outlines *what* needs to be done
  - Not *how* to do it
- Automated system policies should mirror written policies

تنظیم یک سیاست امنیتی

- یک سیاست امنیتی موارد زیر را تعریف می‌کند:
  - نیازمندی های امنیتی یک سازمان و
  - اقدامات کنترلی و محرومیت هائی که در راستای برآورده ساختن آن نیازمندی ها مورد نیاز هستند.
- یک سیاست امنیتی خوب،
  - مسئولیت ها و رفتاری که از اعضای سازمان انتظار می رود را مشخص می کند.
  - می گوید چه کارهائی باید انجام شوند
    - اما نمی گوید چطور.
- قوانین سیستم خودکار می بایست بتواند سیاست‌های نوشته شده‌ی یک سازمان را انعکاس دهد.
  - بطور مثال اگر یک سیاست نوشته شده عنوان می‌کند که کلمه عبور باید هر ۳۰ روز یک بار تعویض شوند، آنگاه تمامی سیستم‌ها باید به گونه‌ای پیکربندی شوند تا این قانون را بطور اتوماتیک اجرا کنند.

Establishing a Security Policy (cont'd.)

- Trade-off between:
  - Ease of use
  - Increased security
- Areas of concern
  - Email attachments
  - Wireless devices
- VPN uses the Internet to relay communications but maintains privacy through security features
- Additional security includes encrypting originating and receiving network addresses

تنظیم یک سیاست امنیتی (ادامه)

- (در زمان اعمال محدودیت های امنیتی) سبک سنگین کردن بین موارد زیر باید انجام شود:
  - سهولت استفاده
  - امنیت افزایش یافته

  وقتی تصمیم در راستای راحتی استفاده باشد، حوادث امنیتی افزایش می یابد.
- مسائلی که باید (در سیاست امنیتی هر سازمان)در نظر گرفت:
  - پیوست های ایمیل
    - حمله کنندگان می‌توانند با دور زدن فایروال و جنبه‌های امنیتی می‌توانند به شبکه نفوذ کنند
  - استفاده از ابزارهای بی‌سیم
    - استعداد پذیرش ویروس ها و کرم ها هستند و به شبکه سازمان وصل می‌شوند
    - تهدید امنیتی اصلی ازدست دادن یا سرقت دستگاه است.
- VPN با استفاده از اینترنت به ایجاد ارتباط می‌پردازد و حریم را از طریق ویژگیهای امنیتی برقرار می‌کند.
- امنیت اضافه تر شامل رمزگذاری آدرس شبکه های مبدا و مقصد می باشد.

Educating Employees, Contractors, and Part-Time Workers

- Educate and motivate users to understand and follow policy
- Discuss recent security incidents
- Help protect information systems by:
  - Guarding passwords
  - Not allowing sharing of passwords
  - Applying strict access controls to protect data
  - Reporting all unusual activity
  - Protecting portable computing and data storage devices

آموزش کارمندان، پیمانکاران و کارکنان نیمه وقت

- آموزش و انگیزش کاربران به منظور یادگیری و پیروی از سیاست ها
- برای نیل به این هدف باید حوادث امنیتی اخیر را مورد بحث و بررسی قرارداد.
  - کاربران باید درک کنندکه آنها بخش کلیدی یک سیستم امنیتی هستند و مسئولیت های خاص دارند.
- کاربران باید در حفاظت از سیستم‌های اطلاعاتی و داده‌های سازمان با انجام موارد زیر کمک کنند:
  - محافظت از کلمات عبور
  - عدم استفاده مشترک از کلمات عبور
  - اعمال اقدامات کنترلی دسترسی سخت گیرانه برای محافظت از داده ها
  - گزارش تمامی فعالیت های غیر طبیعی
  - محافظت از تجهیزات ذخیره سازی و پردازشی قابل حمل

Prevention

- Implement a layered security solution
  - Make computer break-ins harder
- Installing a corporate firewall
  - Limits network access
- Intrusion prevention systems
  - Block viruses, malformed packets, and other threats
- Installing antivirus software
  - Scans for sequence of bytes or virus signature
  - United States Computer Emergency Readiness Team (US-CERT) serves as clearinghouse

پیشگیری

- پیاده سازی یک راه حل امنیتی لایه لایه
  - مشکل تر کردن نفوذ به کامپیوتر
- نصب یک دیواره آتش سازمانی
  - دسترسی شبکه را بر اساس سیاست دسترسی سازمان محدود می سازد
- سیستم های جلوگیری از نفوذ
  - ویروس ها، بسته های بدفرم و دیگر تهدیدات را بلاک می کند.
- نصب نرم افزار ضد ویروس
  - پویش نمودن حافظه و دیسک درایوهای کامپیوتر برای دنباله مشخصی از بایت‌ها یا امضای ویروس

Prevention (cont'd.)

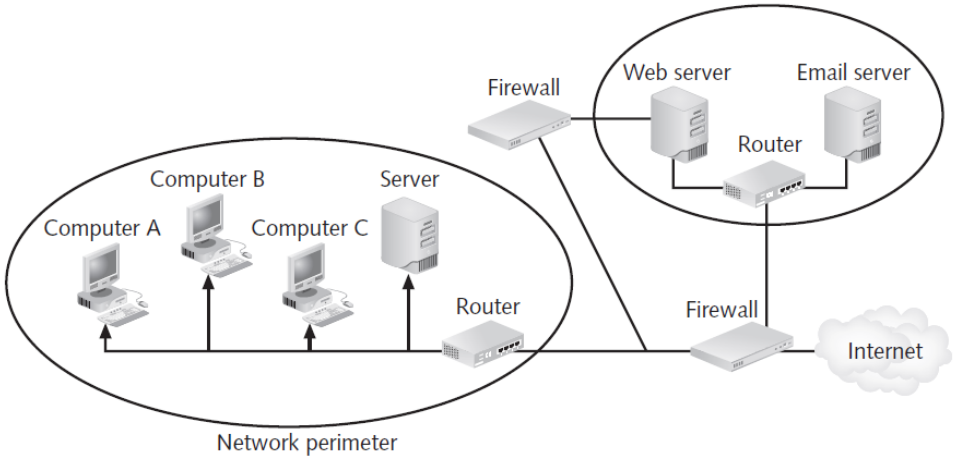

FIGURE 3-6 Firewall
Source Line: Course Technology/Cengage Learning.

پیشگیری (ادامه)

دیواره آتش

Prevention (cont'd.)

TABLE 3-8 Popular firewall software for personal computers

Software	Vendor
Zone Alarm Pro	CheckPoint Software Technologies Ltd.
F-Secure Internet Security	F-Secure Corporation
Panda Global Protection	Panda Security
NeT Firewall	NT Kernel Resources
ESET Smart Security 4	ESET

Source Line: "Best Firewall Software–Editor's Choice," All-Internet-Security.com, © January 2011, www.all-internet-security.com/top_10_firewall_software.html.

پیشگیری (ادامه)

- **نرم افزارهای معروف دیواره آتش برای کامپیوترهای شخصی**

Prevention (cont'd.)

- Safeguards against attacks by malicious insiders
- Departing employees and contractors
  - Promptly delete computer accounts, login IDs, and passwords
- Carefully define employee roles and separate key responsibilities
- Create roles and user accounts to limit authority

پیشگیری (ادامه)

- **به کارگیری حفاظ ها در برابر حملات نفوذی های بدخواه**
- **کارمندان و پیمانکارانی که سازمان را ترک می کنند**
  - **حذف سریع حساب های کامپیوتری، IDهای ورودی و کلمات عبور**
- **تعریف دقیق نقش کارمندان و جداسازی مسئولیت های کلیدی**
- **ایجاد نقش ها و حساب های کاربری محدود برای اجرای مسئولیتهای مربوطه و نه بیشتر**

Prevention (cont'd.)

- Defending against cyberterrorism
  - Department of Homeland Security and its National Cyber Security Division (NCSD) is a resource
    - Builds and maintains a national security cyberspace response system
    - Implements a cyber-risk management program for protection of critical infrastructure, including banking and finance, water, government operations, and emergency services

پیشگیری (ادامه)

Prevention (cont'd.)

- Conduct periodic IT security audits
  - Evaluate policies and whether they are followed
  - Review access and levels of authority
  - Test system safeguards
  - Information Protection Assessment kit is available from the Computer Security Institute

پیشگیری (ادامه)

- **اجرای بازرسی‌های دوره ای امنیت IT**
  - **ارزیابی کردن اینکه آیا یک سازمان، سیاست امنیتی درستی دارد و اینکه آیا این سیاست دنبال می‌شود.**
  - **بازرسی دسترسی‌ها و سطوح مجوزها و اختیارات**
  - **آزمایش حفاظ های امنیتی**

Detection

- Detection systems
  - Catch intruders in the act
- Intrusion detection system
  - Monitors system/network resources and activities
  - Notifies the proper authority when it identifies:
    - Possible intrusions from outside the organization
    - Misuse from within the organization
  - Knowledge-based approach
  - Behavior-based approach

کشف

- سیستم های کشف
  - به دام انداختن نفوذ گران در حین ارتکاب عمل
- سیستم کشف نفوذ
  - نرم افزار و/یا سخت افزاری است
  - نظارت و کنترل فعالیت ها و منابع سیستم/شبکه
  - هرگاه موارد زیر را شناسائی کند ، عوامل شبکه مطلع می سازد:
    - نفوذی های احتمالی خارج از سازمان
    - سوء استفاده از داخل سازمان
- راهکارهای کشف نفوذ
  - راهکار دانش بنیان
    - مراقب اقداماتی است که جهت سوء استفاده از از نقاط آسیب پذیر از قبل شناخته شده صورت می پذیرند.
  - راهکار رفتار-محور
    - مقایسه رفتار طبیعی سیستم ها و کاربرانشان با فعالیت فعلی آنها و در صورت شناسائی انحراف، اعلام هشدار

Response

- Response plan
  - Develop well in advance of any incident
  - Approved by:
    - Legal department
    - Senior management
- Primary goals
  - Regain control and limit damage
  - Not to monitor or catch an intruder
- Only 56% have response plan

پاسخ

- **طرح پاسخ**
  - **باید پیش از رخداد هر حادثه ای به خوبی ایجاد شود**
  - **و توسط ...**
    - **اداره قانون سازمان**
    - **و مدیریت ارشد**

    مورد تایید قرار گیرد.
- **اهداف اصلی در هر حادثه امنیتی**
  - **بدست آوردن دوباره کنترل و محدود کردن خسارات**
  - **نباید تلاشی برای نظارت یا گیر انداختن اخلال گر صورت گیرد.**
- **تنها ۵۶ درصد سازمان ها دارای طرح پاسخ هستند.**

Response (cont'd.)

- Incident notification defines:
  - Who to notify
  - Who not to notify
- Security experts recommend against releasing specific information about a security compromise in public forums
- Document all details of a security incident
  - All system events
  - Specific actions taken
  - All external conversations

پاسخ (ادامه)

- **اطلاع رسانی حادثه**
  - **(در طرح پاسخ) اطلاع رسانی حادثه بیان می کند که**
    - **چه کسی باید مطلع شود.**
    - **چه کسی نباید مطلع شود.**
  - **متخصصین امنیت، عدم انتشار اطلاعات خاص حول خطرات امنیتی را در انجمن‌های عمومی توصیه می‌کنند.**

- **حفاظت از شواهد و ثبت فعالیت ها**
  - **(هر سازمان باید) تمامی جزییات یک حادثه امنیتی را در حین تلاش برای مرتفع سازی آن مستند کند.**

    - **جمع آوری تمامی رخدادهای سیستم**
    - **عملیات خاص اتخاذ شده (چه چیزی، چه زمانی و چه کسی)**
    - **تمامی مکالمات خارجی (چه چیزی، چه زمانی و چه کسی)**
  - **مستند سازی**
    - **شواهد ارزشمندی را برای پیگردی‌های آتی گردآوری می‌کند**
    - **و داده‌هائی را برای کمک در خلال ریشه کن سازی حادثه و فاز پیگیری فراهم می آورد.**

-

Response (cont'd.)

- Act quickly to contain an attack
- Eradication effort
  - Collect and log all possible criminal evidence
  - Verify necessary backups are current and complete
  - Create new backups
- Follow-up
  - Determine how security was compromised
    - Prevent it from happening again

پاسخ (ادامه)

- **کنترل وجلوگیری از حادثه**
  - **باید سریع عمل کرد تا جلوی یک حمله را گرفت (و موقعیت بد را از بدتر شدن حفظ کرد).**
- **ریشه کن سازی**
  - **پیش از آنکه تلاش برای ریشه کن سازی آغاز شود باید**
    - **تمامی شواهد جزایی احتمالی جمع آوری و ثبت گردد**
    - **اینکه پشتیبان های لازم حاضر و کامل باشد بررسی گردد**
    - **پشتیبان های جدید تهیه کرد تا برای مطالعات بعدی یا به عنوان شواهد بتواند مورد استفاده قرار گیرد.**
  - **پس از ریشه کن سازی باید یک فایل پشتیبان جدید تهیه شود.**
  - **در سراسر فرآیند باید یک فایل ثبت برای تمامی اعمال اتخاذ شده نگهداری شود.**
- **پیگیری**
  - **معلوم می کند که امنیت چگونه به خطر افتاده است.**
    - **از اتفاق افتادن مجدد حادثه جلوگیری می کند.**

Response (cont'd.)

- Review
  - Determine exactly what happened
  - Evaluate how the organization responded
- Weigh carefully the amount of effort required to capture the perpetrator
- Consider the potential for negative publicity
- Legal precedent
  - Hold organizations accountable for their own IT security weaknesses

پاسخ (ادامه)

- **بازبینی**
  - **باید پس از یک حادثه صورت گیرد**
  - **اینکه چه اتفاقی روی داده است را مشخص می کند.**
  - **اینکه سازمان چگونه به حادثه پاسخ داده است را ارزیابی می کند.**
  - **تخمین خسارات مالی**
    - **از دست رفتن عایدی ها**
    - **از دست رفتن سود ناشی از به سرقت رفتن رازهای شرکت**
    - **افت بازدهی**
    - **حقوق افرادی که در راستای مرتفع سازی حادثه کار می کنند**
    - **هزینه تعویض داده ها، نرم افزار و سخت افزار**
    - **سنجیدن دقیق میزان تلاش مورد نیاز برای به دام انداختن مرتکب جرم**
  - **پتانسیلی که برای شهرت منفی وجود دارد را نیز باید در نظر گرفت.**
  - **حتی اگر یک شرکت به این نتیجه برسد که خطر شهرت منفی وجود ندارد و به مرتکب آن مربوط می‌شود، سندهای حاوی اطلاعات اختصاصی که می‌بایست در دادگاه ارائه شود م تواند یک تهدید امنیتی بزرگ ایجاد کند.**
  - **باید شرکت تصمیم بگیرد که آیا اصول اخلاقی یا وظیفه قانونی مبنی بر مطلع سازی مشتریان را دارد یا خیر؟**

Computer Forensics

- Combines elements of law and computer science to identify, collect, examine, and preserve data and preserve its integrity so it is admissible as evidence
- Computer forensics investigation requires extensive training and certification and knowledge of laws that apply to gathering of criminal evidence

Summary

- Ethical decisions in determining which information systems and data most need protection
- Most common computer exploits
  - Viruses
  - Worms
  - Trojan horses
  - Distributed denial-of-service attacks
  - Rootkits
  - Spam
  - Phishing, spear-fishing, smishing, vishing

Summary (cont'd.)

- Perpetrators include:
  - Hackers
  - Crackers
  - Malicious insider
  - Industrial spies
  - Cybercriminals
  - Hacktivist
  - Cyberterrorists

Summary (cont'd.)

- Must implement multilayer process for managing security vulnerabilities, including:
  - Assessment of threats
  - Identifying actions to address vulnerabilities
  - User education
- IT must lead the effort to implement:
  - Security policies and procedures
  - Hardware and software to prevent security breaches
- Computer forensics is key to fighting computer crime in a court of law