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 اول
  - جرایم کامپیوتری و اینترنتی
- هفته هفتم
  - نیمسال دوم ۹۲-۹۳

SMS : 0939 – 101 0024
eMail : EIT @ EXIST . IR

Objectives

- As you read this chapter, consider the following questions:
  - What key trade-offs and ethical issues are associated with the safeguarding of data and information systems?
  - Why has there been a dramatic increase in the number of computer-related security incidents in recent years?
  - What are the most common types of computer security attacks?

اهداف

- **همچنانکه این فصل را می خوانید، پرسش های زیر را نیز در نظر بگیرید:**
  - **چه مسائل اخلاقی و سبک-سنگین کردن های کلیدی با حفاظت از داده ها و سیستم های اطلاعاتی مرتبط است؟**
  - **چرا افزایش چشمگیری در تعداد رویدادهای امنیتی مرتبط با کامپیوتر در سال های اخیر وجود داشته است؟**
  - **رایج ترین انواع حملات امنیتی کامپیوترها کدام هستند؟**

Objectives (cont'd.)

- Who are the primary perpetrators of computer crime, and what are their objectives?
- What are the key elements of a multilayer process for managing security vulnerabilities based on the concept of reasonable assurance?
- What actions must be taken in response to a security incident?
- What is computer forensics, and what role does it play in responding to a computer incident?

اهداف – ادامه

- **مرتکبین اصلی جرایم کامپیوتر چه کسانی هستند، و اهداف آن ها چیست؟**
- **عناصر کلیدی یک فرآیند چند لایه برای مدیریت نقاط آسیب پذیر امنیتی بر اساس مفهوم تضمین معقول کدام ها هستند؟**
- **چه عملیاتی می بایست در پاسخ به یک رویداد امنیتی اتخاذ شوند؟**

IT Security Incidents: A Major Concern

- Security of information technology is of utmost importance
  - Safeguard:
    - Confidential business data
    - Private customer and employee data
  - Protect against malicious acts of theft or disruption
  - Balance against other business needs and issues
- Number of IT-related security incidents is increasing around the world

رویداد های امنیتی فناوری اطلاعات: یک نگرانی مهم

- **امنیت فناوری اطلاعات (به کار رفته در کسب وکار) دارای اهمیت بسیار بالایی است.**
  - **از موارد زیر حفاظت می کند :**
    - **داده های محرمانه کسب وکار**
    - **اطلاعات خصوصی مشتریان و کارکنان**
  - **از (سیستم ها) در مقابل اعمالی همچون سرقت یا ایجاد اختلال که توام با سوء نیت هستند محافظت می کند.**
  - **در برابر نیازها و مسائل مربوط به کسب و کار باید به تعادل برسد**
  - **تعداد رویدادهای امنیتی مرتبط با فناوری اطلاعات در سراسر دنیا در حال افزایش است.**

Why Computer Incidents Are So Prevalent

- Increasing complexity increases vulnerability
  - Computing environment is enormously complex
    - Continues to increase in complexity
    - Number of entry points expands continuously
    - Cloud computing and virtualization software
- Higher computer user expectations
  - Computer help desks under intense pressure
    - Forget to verify users' IDs or check authorizations
- Computer users share login IDs and passwords

چرا رویدادهای کامپیوتری بسیار شایع شده اند

- پیچیدگی روبه افزایش، آسیب پذیری را افزایش می دهد.
  - محیط پردازشی تا حد زیادی پیچیده می باشد.
    - این محیط دائم به پیچیدگی خود می افزاید
      - شبکه ها، کامپیوترها، سیستم های عامل، برنامه ها، وب سایت ها، سوییچ ها، روترها، گیت وی ها
    - تعداد نقاط ورود به شبکه به طور مداوم در حال گسترش است.
    - افزایش به کارگیری رایانش ابری و نرم افزارهای مجازی سازی
  - انتظارات بیشتر کاربری کامپیوتر
  - افراد Help Desk کامپیوتر(برای پاسخ به پرسش های کاربران) تحت فشار شدیدی هستند.
    - بطور مثال گاهی فراموش می کنند هویت کاربران را تایید کنند یا مجوزهای دسترسی را چک کنند.
  - کاربران کامپیوتر نام کاربری و کلمه عبور خود را با دیگر همکاران به اشتراک می گذارند.

Why Computer Incidents Are So Prevalent (cont'd.)

- Expanding/changing systems equal new risks
  - Network era
    - Personal computers connect to networks with millions of other computers
    - All capable of sharing information
  - Information technology
    - Ubiquitous
    - Necessary tool for organizations to achieve goals
    - Increasingly difficult to match pace of technological change

چرا رویدادهای کامپیوتری بسیار شایع شده اند – ادامه

- **توسعه و تغییر سیستم ها خطرات جدیدی را بدنبال دارد.**
  - **عصر شبکه**
    - **کامپیوترهای شخصی به شبکه هائی با میلیون ها کامپیوتر متصل می شوند.**
    - **که همه قادر به اشتراک گذاری اطلاعات می باشند.**
  - **فناوری اطلاعات**
    - **فراگیر**
    - **ابزاری ضروری برای سازمان ها جهت نیل به اهداف**
    - **همراه شدن با سرعت تغییرات تکنولوژی بطور فزاینده ای دشوار می باشد.**

Why Computer Incidents Are So Prevalent (cont'd.)

- Increased reliance on commercial software with known vulnerabilities
  - Exploit
    - Attack on information system
    - Takes advantage of system vulnerability
    - Due to poor system design or implementation
  - Patch
    - "Fix" to eliminate the problem
    - Users are responsible for obtaining and installing
    - Delays expose users to security breaches

چرا رویدادهای کامپیوتری بسیار شایع شده اند – ادامه

- اتکای فزاینده بر نرم افزارهای تجاری با آسیب پذیری های شناخته شده
  - بهره کشی یا سوء استفاده
    - حمله ای است به یک سیستم اطلاعاتی
    - که به سبب طراحی یا پیاده سازی ضعیف سیستم
    - از آسیب پذیری های سیستم بهره برداری می کند
  - وصله
    - تعمیری است جهت رفع مشکل
    - کاربران سیستم مسئول دریافت و نصب وصله هستند
    - هر گونه تاخیر در نصب وصله، کاربر را در معرض یک رخنه امنیتی قرار می دهد.

Why Computer Incidents Are So Prevalent (cont'd.)

- Zero-day attack
  - Before a vulnerability is discovered or fixed
- U.S. companies rely on commercial software with known vulnerabilities

چرا رویدادهای کامپیوتری بسیار شایع شده اند – ادامه

- **حمله صفر روز**
  - **پیش از آنکه آسیب پذیری (توسط توسعه گران نرم افزار یا انجمن امنیت) سیستم کشف گردد یا برطرف شود اتفاق می افتد.**
- **لذا شرکت های ایالات متحده بر نرم افزارهای تجاری با آسیب پذیری های شناخته شده تکیه دارند.**

Types of Exploits

- Computers as well as smartphones can be target
- Types of attacks
  - Virus
  - Worm
  - Trojan horse
  - Distributed denial of service
  - Rootkit
  - Spam
  - Phishing (spear-phishing, smishing, and vishing)

انواع بهره کشی

- کامپیوترها و همچنین تلفنهای هوشمند می توانند هدف بهره کشی باشند.
- انواع حمله
  - ویروس
  - کرم
  - اسب تروجان
  - انکار سرویس توزیع شده
  - روتکیت
  - بات نت
  - اسپم
  - فیشینگ(نیزه ای، اسمیشینگ و ویشینگ)

Viruses

- Pieces of programming code
- Usually disguised as something else
- Cause unexpected and undesirable behavior
- Often attached to files
- Deliver a “payload”
- Spread by actions of the “infected” computer user
    - Infected e-mail document attachments
    - Downloads of infected programs
    - Visits to infected Web sites

ویروس

- **تکه ای از کد برنامه نویسی است**
- **معمولا در قالب چیز دیگری پنهان می شود**
- **باعث رفتاری غیرقابل انتظار و معمولا نا خوشایندی می شود**
- **اغلب به یک فایل پیوست می شود(که وقتی فایل باز می شود اجرا می گردد)**
- **یک تاثیر مخرب ارائه می کند**
- **با اعمال کاربر کامپیوتر آلوده پخش می شود**
    - **باز کردن پیوستهای آلوده ایمیل**
    - **بارگذاری برنامه های آلوده**
    - **بازدید وب سایت های آلوده**

Worms

- Harmful programs
  - Reside in active memory of a computer
  - Duplicate themselves
- Can propagate without human intervention
- Negative impact of worm attack
  - Lost data and programs
  - Lost productivity
  - Additional effort for IT workers

کرم

- **برنامه های آسیب زننده و مضر**
  - **در حافظه فعال کامپیوتر مقیم می شود**
  - **خود را تکثیر می کند**
- **بدون مداخله انسان می تواند انتشار یابد**
- **تاثیر منفی حمله کرم**
  - **از دست دادن داده ها و برنامه ها**
  - **از دست رفتن بازدهی به دلیل عدم توانائی کارکنان در استفاده از کامپیوتر**
  - **تلاش مازاد کارکنان فناوری اطلاعات(برای بازیابی داده ها و برنامه ها و پاکسازی آلودگی)**

Trojan Horses

- Malicious code hidden inside seemingly harmless programs
- Users are tricked into installing them
- Delivered via email attachment, downloaded from a Web site, or contracted via a removable media device
- Logic bomb
  - Executes when triggered by certain event

×

اسب تروا

- **کدهای مخرب مخفی شده در یک برنامه به ظاهر بی ضرر**
- **کاربران اغلب گول می خورند و تروجان را نصب می کنند**
- **از طریق پیوست ایمیل، بارگذاری از یک وب سایت یا از طریق یک رسانه قابل حمل پخش می گردد.**
- **بمب منطقی**
  - **وقتی یک رویداد خاص اتفاق می افتد اجرا می شود.**

Distributed Denial-of-Service (DDoS) Attacks

- Malicious hacker takes over computers on the Internet and causes them to flood a target site with demands for data and other small tasks
  - The computers that are taken over are called zombies
  - Botnet is a very large group of such computers
- Does not involve a break-in at the target computer
  - Target machine is busy responding to a stream of automated requests
  - Legitimate users cannot access target machine

حملات انکار سرویس توزیع شده

- حمله ای است که در آن یک هکر بدخواه از طریق اینترنت، کنترل کامپیوترها را به دست گرفته و باعث می شود که به یک سایت هدف سرازیر شوند و درخواست داده ها یا کارهای کوچک دیگر بکنند.
- کامپیوترهائی که تحت کنترل قرار می گیرد ، زامبی نامیده می شود.
- بات نت گروه بزرگی از کامپیوترها است که توسط هکرها از یک یا چند مکان راه دور بدون آنکه راهبران یا دارندگان آن آگاه یا راضی باشند کنترل می شوند و می توانند همان زامبی ها باشند.
- شامل وقفه در کامپیوتر مقصد نیست بلکه
  - هدف را آنقدر مشغول پاسخ دهی به سیلی از درخواست های اتوماتیک نگاه می دارد
  - که کاربران اصلی و قانونی قادر به ورود به سیستم نباشند.

Rootkits

- Set of programs that enables its user to gain administrator-level access to a computer without the end user's consent or knowledge
- Attacker can gain full control of the system and even obscure the presence of the rootkit
- Fundamental problem in detecting a rootkit is that the operating system currently running cannot be trusted to provide valid test results

روتکیت

- ✕ **مجموعه ای از برنامه ها است که به کاربر خود اجازه دسترسی سطح مدیر را به یک کامپیوتر می دهد بدون آنکه کاربر هائی آگاه بوده یا راضی باشد**
- ✕ **حمله کننده می تواند کنترل کاملی ازسیستم داشته باشدو حتی حضور روتکیت را از مدیران قانونی سیستم مخفی نگاه دارد**
- ✕ **مشکل اساسی در تشخیص یک روتکیت آن است که نمی توان به سیستم عاملی که حالت اجرا است اعتماد کرد، چرا که نتایج آزمایشی معتبری را به دست نمی دهد**

Spam

- Abuse of email systems to send unsolicited email to large numbers of people
  - Low-cost commercial advertising for questionable products
  - Method of marketing also used by many legitimate organizations
- Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act
  - Legal to spam if basic requirements are met

اسپم

Spam (cont'd.)

- Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA)
  - Software generates tests that humans can pass but computer programs cannot

Phishing

- Act of using email fraudulently to try to get the recipient to reveal personal data
- Legitimate-looking emails lead users to counterfeit Web sites
- Spear-phishing
  - Fraudulent emails to an organization's employees
- Smishing
  - Phishing via text messages
- Vishing
  - Phishing via voice mail messages

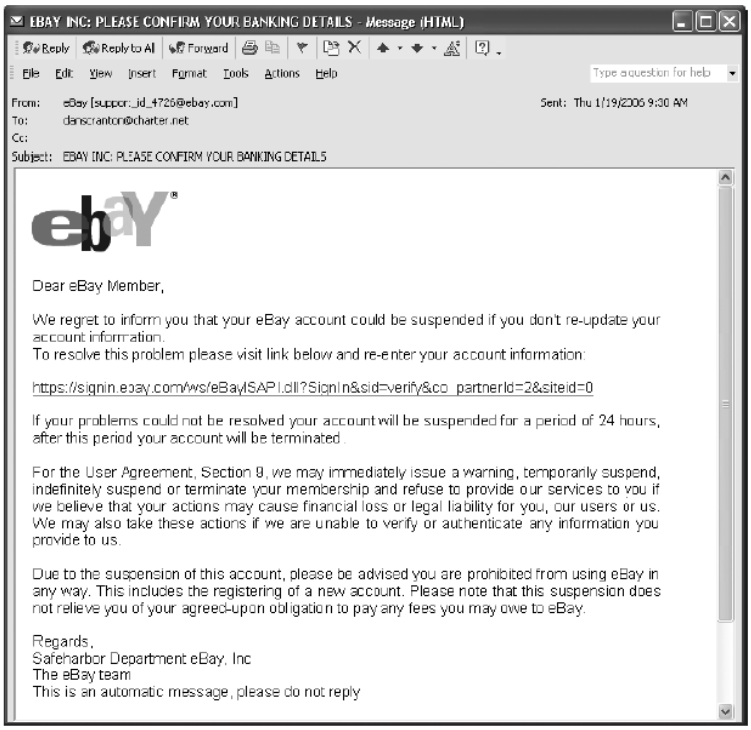

FIGURE 3-3 Example of phishing
Source Line: Course Technology/Cengage Learning.