Microsoft TWC

Trustworthy Computing

Vortrag von: Rui Deng
Sven Schneeberg
Adrian Detlefs
Marius Loska

Übersicht

Geschichte

Ziele

Framework von TWC

Sicherheitsphilosophie (vier Aspekte)

Geschichte

Idee von Bill Gates:

> „*Die computerbetriebenen Geräte sollen selbstverständlich und einfach nutzbar sein, wie die heutigen elektrischen Geräte.“*

50000 Mitarbeiter sollen sich mit der Idee befassen.

Sicherheit in einer vernetzten Welt.

Geschichte

Sofortige Maßnahmen:

- Microsoft stoppt die Entwicklungsarbeit.
- 8500 Microsoft Entwickler besuchen Sicherheitsschulung.
- Lernen von neuen Entwurfsmethoden, Programmierpraktiken und Testverfahren.

Geschichte

“Trustworthy Computing is the highest priority for all the work we are doing. We must lead the industry to a whole new level of Trustworthiness in computing.”
– Bill Gates, 15 January 2002


Trustworthy Computing
Security
Privacy
Reliability
Business Integrity

Trustworthy Computing

Security

Der Kunde erwartet das sein System sicher gegen Angreifer ist.

Privacy

Die Kunden sollen selber in der Lage sein über ihre Daten zu verfügen.

Reliability

Der Kunde erwartet alle vom System zu Verfügung stehenden Funktionen.

Business Integrity

Bei Problemen, dem Kunden entgegenkommen und ihm effektiv und schnell helfen.

Framework von TWC

Secure by Design (Sicherheit im Konzept)

Secure by Default (Sicherheit als Standard)

Secure by Deployment (Sicherheit bei der Bereitstellung)

Communication (Kommunikation)


SD³ + Communications
Secure by Design
Sicherheit schon während des Designprozesses
Secure by Default
Funktionen sind bei der Auslie-ferung einer Software deaktiviert
Secure in Deployment
Kunden bekommen Tools und Services
Communications
Microsoft sucht den Dialog mit seinen Kunden

Secure By Design

Microsoft Trustworthy Computing

Adrian Detlefs

Übersicht

- Spezielle Probleme für Microsoft
- Allgemeine Probleme der SW-Entwicklung
- Maßnahmen
- Neue Tools
- Microsoft Driver Framework

Spezielle Probleme für Microsoft

- rasantes Wachstum des Internets
- neue potentielle Angreifer
- ‚Soft-Target' durch marktbeherrschende Stellung
- neue Features mussten integriert werden
- Internet-Technologien, die ihrerseits Sicherheitslücken mitbringen

Weitere Probleme:

- MS Produkte sollten möglichst alle denkbaren Features unterstützen
- Hardwarevielfalt der PC-Plattform
- schlecht programmierte Treiber der Hersteller

→ es entstanden mehr Sicherheitslücken als erwartet

Allgemeine Probleme der SW-Entwicklung

Neben der Softwarearchitektur hat der Programmierer folgende Punkte zu beachten:

- Performanz
- Wartbarkeit
- Speichermanagement
- Parallelverarbeitung
- Lokalisierung

→ Bei der Implementierung können zahlreiche Fehler auftreten

Maßnahmen

- Security-Training
  - intensives Training für 8500 Windows-Entwickler und Analyse des vorhandenen Windows Codes
  - Threat Modeling, Sicheres Programmieren, Testverfahren
- Threat Modeling
  - Anwenden von Angriffen auf eine Komponente noch während des Designs
  - Ableitung von Strategien zur Sicherung der Komponente gegen Bedrohungen
    → 50% der Fehler konnten durch Threat Modeling gefunden werden
- Code Review
  - Auffinden der problematischsten Stellen durch Threat Modeling
  - fehlerhafter Code aus älteren Programmversionen wurde identifiziert
- Anwendung der Erkenntnisse auf andere SW-Projekte

Tools

- Threat Modeling Tool (noch in Arbeit)
  - soll beim Modellieren und Beschreiben von Bedrohungen helfen
- FxCop
  - Einhaltung von .NET Design Richtlinien
  - Namenskonventionen
  - Performance
  - Lokalisierung
- Writing Secure Code von Michael Howard und David LeBanc
  - Buch über die Entwicklung sicherer Software

Windows Driver Framework

- Beschreibt ein Rahmenwerk für zukünftige Windows Treiber
- wird einfließen in Windows „Longhorn“
- Erstellung von Hardware-Treibern anhand von Bibliotheken und Vorlagen

→ Hardwarehersteller sollen weniger Fehler bei der Erstellung von Treibern machen

Secure in Deployment

Microsoft Trustworthy Computing

200223912

Rui Deng

Übersicht

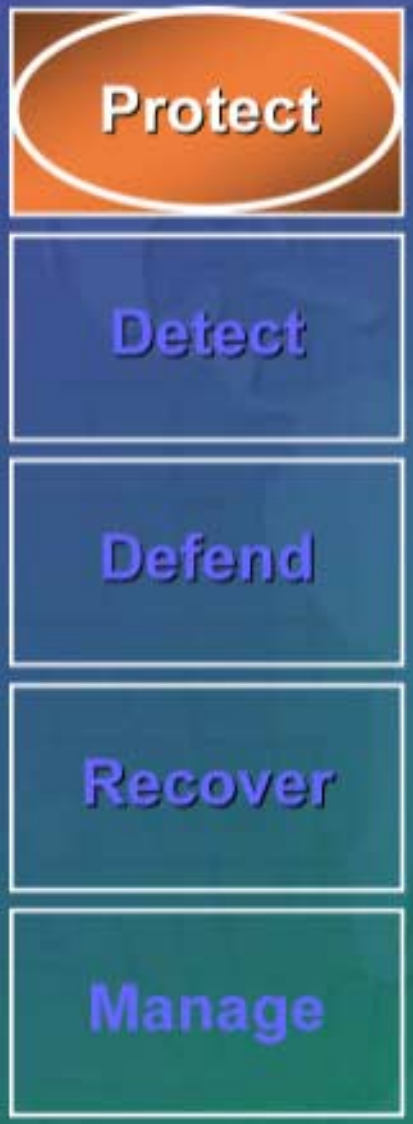
- Der Grundgedanke von „Secure in Deployment“
- Aktueller Entwicklungsstand bei Microsoft

Secure in Deployment

Sicherheit bei der Bereitstellung

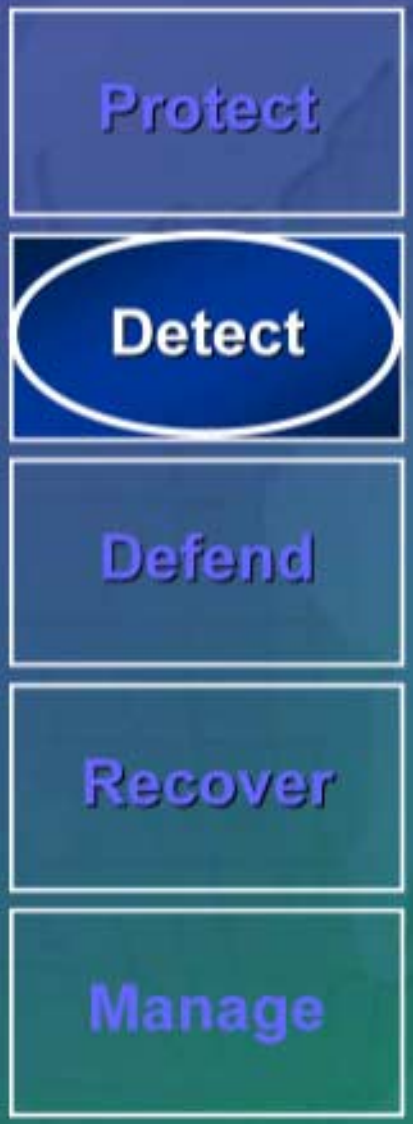
- Protect
- Detect
- Defend
- Recover
- Manage

Secure in Deployment : Protect



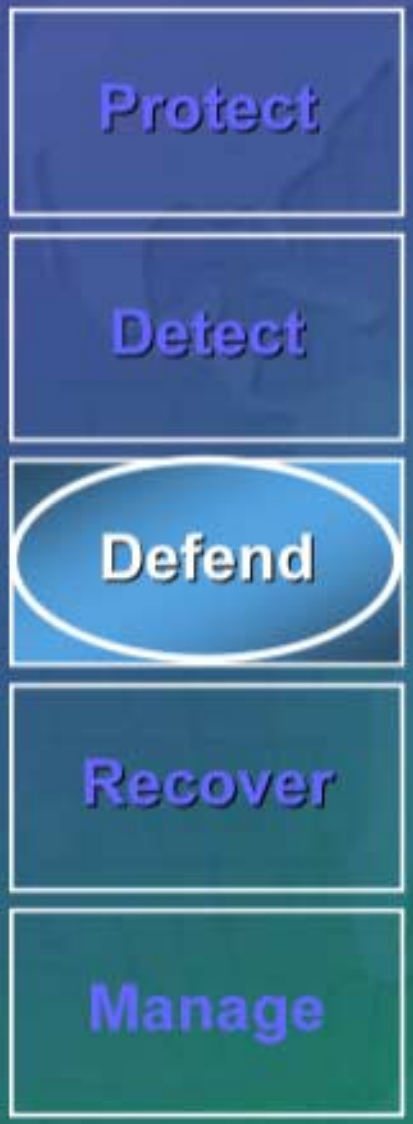
- Systeme schützen
- Daten sind nur vertrauenswürdigen Benutzern verfügbar
- Die Systeme sind vernünftig konfiguriert
- Die Systeme werden gewartet um unbefugten Zugriff zu vermeiden
- Schutz von Netzwerk ist so ähnlich wie die Schließung der Tür, damit man sein Zuhause gegen einen Einbrecher verteidigen kann.

Secure in Deployment : Detect



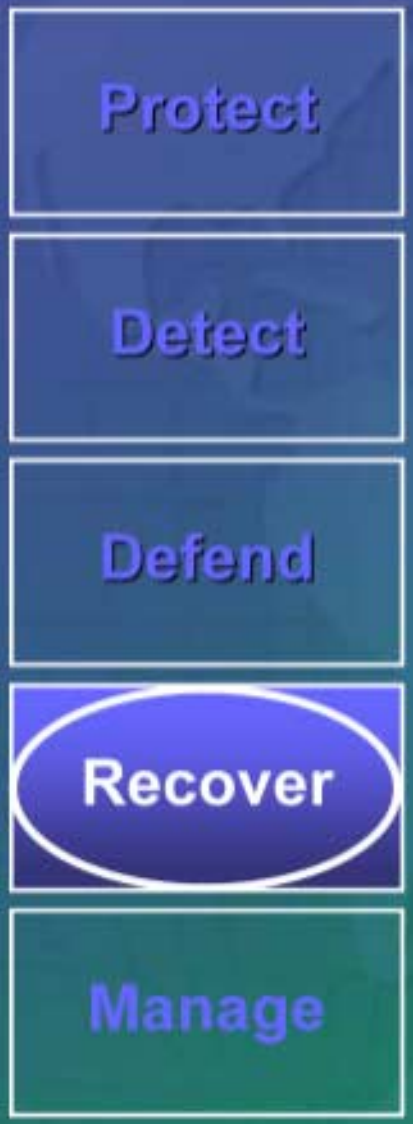
- Erkennen von Einbruchsversuchen, Verletzungen der Sicherheit, Betriebsprobleme, unerwarteten Verhaltensweisen der Systeme oder Indizien von möglichen neuen Fehlern.
- Erkennung ist analog zu dem Aktivieren des Alarmes, damit man vor dem Angriff gewarnt werden kann.

Secure in Deployment : Defend



- Verteidigen der Systeme durch automatisierte Korrektur des Fehlers wenn ein Sicherheits-problem aufgetreten ist oder vermutet wird.
- Man kann das auch wie mit dem Rufen der Polizei während eines Angriffs vergleichen.

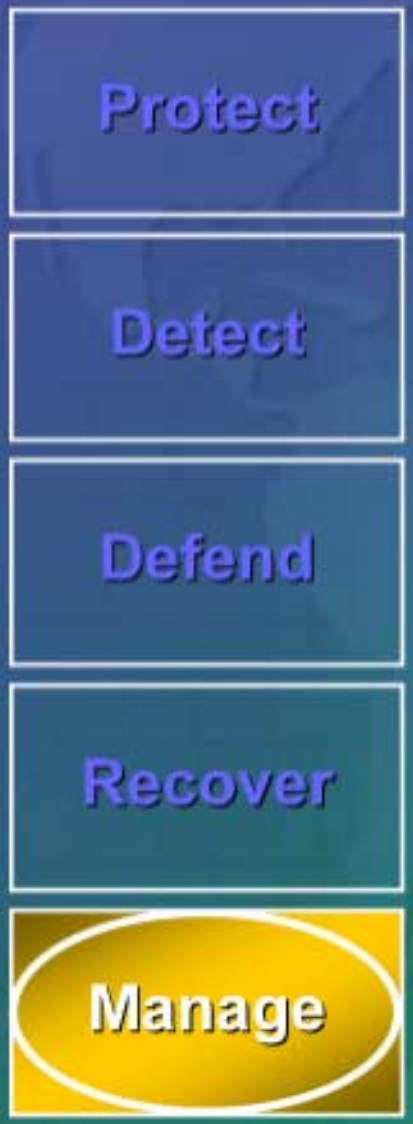
Secure in Deployment : Recover



- Wiederherstellen der Systeme:
  Im Informatik Bereich (IT) mit einem Backup-System kann man ein infiziertes System schnell auf den guten Urzustand zurückbringen.

- Wiederherstellen ist so ähnlich wie das Rufen einer Versicherungsfirma, um nach einem Angriff den Schaden erstattet zu bekommen.

Secure in Deployment : Manage



- Definieren von Regeln, um künftige Bedrohungen entgegenzutreten
- Sicherheitsmanagementvorgänge können automatisiert werden
- Systeme können konfiguriert werden
- Administrator wird alarmiert wenn Sicherheitsverletzungen erkannt werden oder z.B. der Zuständigkeits-bereich von Usern überschritten wird.

Progress to Date

- Die Ausbildung der Administratoren ist absolut wichtig.
- Die meisten Firmen sparen kräftig in diesen Bereichen.
- Microsoft hat ein neues sicherheitsfokussiertes Training initiiert, die von Microsoft Certified Technical Education Centers (CTECs) und Authorized Academic Training Partners (AATPs) geleitet wird.

Progress to Date

- Das kostenlose Online Microsoft Security Toolkit
- Security Operations Guide für Windows 2000 Server
- Der kostenlose Telefon-support im Falle des Angriffs von Viren

Progress to Date

- Tools: „ Microsoft Baseline Security Analyzer (MBSA)”
- Automatisches Updatefeature in den meisten Versionen von Microsoft Windows
- Microsoft Software Update Service (SUS)
- Systems Management Server (SMS)
- „Microsoft Internet Security and Acceleration (ISA) Server 2000”

Secure By Default

Microsoft Trustworthy Computing

Sven Schneeberg

Probleme

- Microsoft unterstützt viele nicht benutzte Features
- Das Internet ist unerwartet schnell gewachsen
- Hacker Tools erlauben es jedem Angriffe starten

Ziele

- Reduzierung der Angriffsfläche
  - Weglassen von Terminal Programmen
- Deaktivieren aller gefährdeten Features
  - IE Java Script, ActiveX,..
  - Office VBA Makros (besonders Outlook)
- Niedrigere Priorität für unsichere Programme
  - Nicht als Administrator surfen
  - Programme im „User Mode“ ausführen

Umsetzung

- SUS (Software Update Server)
- Deaktivierung unsicherer Funktionen
- Aktivieren von Sicherheitsprogrammen
- Verbessern der Sicherheitssoftware
- Vereinfachen der Sicherheitsprogramme

Comuncation

Microsoft Trustworthy Computing

Sven Schneeberg

Probleme

- Benutzer wissen nicht das es Sicherheitslücken gibt
- Schon lange vorhandene Patches werden nicht genutzt
- Den Benutzern ist die Wichtigkeit von Sicherheitsprogrammen nicht bewusst

Ziele

- Informationen schnell veröffentlichen wenn Fehler gefunden wurden
- Patches schnell und gezielt an die Benutzer verteilen
- Beratung der Kunden, so dass sie eine hohe Sicherheit ihres Systems erreichen

Umsetzung

- MSRC (Microsoft Security Research Center)
- Beantworten jeder Meldung innerhalb von 24 Sunden, 7 Tage die Woche
- Gespräche mit Benutzern um die Software weiter optimieren zu können
- Bereitstellen von Lösungen zur Benachrichtigung der Benutzer
  - E-Mail Listen
  - Foren
  - Call Center

Ende

Vielen Dank für Ihre Aufmerksamkeit !

Noch Fragen?