Universität Rostock

Traditio et Innovatio

Systemsicherheit am ITMZ

Systemsicherheit am ITMZ

Agenda

- Wie konfiguriere ich ein sicheres und robustes System?
- Stand der Sicherheit bei aktuellen Windows-Systemen – das Positive, das Negative und das „Hässliche“
- Konfigurations-Toolkits für Windows

Systemsicherheit am ITMZ

Grundhaltung - Langfristige Sicherheitsstrategie bedeutet Kombination verschiedener Schutzmechanismen

- Isolierter Einsatz von Netzwerkfirewalls stellt keine Systemsicherheit her
- Alleiniger Einsatz von Anti-Virus Software stellt keine Systemsicherheit her
- Jedes System muss sich selbst schützen können
- Hauptaugenmerk muss auf der sicheren Konfiguration der zu schützenden Endsysteme liegen

Universität Rostock

Traditio et Innovatio

Systemsicherheit am ITMZ

- *Wie konfiguriere ich ein sicheres und robustes System?*

Systemsicherheit am ITMZ

Wie konfiguriere ich ein sicheres und robustes System?

- Grundthese:
  - Je eingeschränkter Programmvielfalt, Netzwerkverkehr und Zugriffsrechte, je mehr Sicherheit.
- Ziel:
  - Kontrolle über das System

Systemsicherheit am ITMZ

Wie konfiguriere ich ein sicheres und robustes System?

- Grundthese:
  - Je eingeschränkter Programmvielfalt, Netzwerkverkehr und Zugriffsrechte, je mehr Sicherheit.
- Umsetzung durch drei Konfigurationsänderungen:
  - Versiegeln - Programmvielfalt einschränken.
  - Isolieren - Netzwerkverkehr einschränken.
  - Herabstufen - Administrative Rechte einschränken.

Systemsicherheit am ITMZ

Wie konfiguriere ich ein sicheres und robustes System?

Drei grundlegende Konfigurationsänderungen

1. **Versiegeln** per Software Whitelisting:

   Programme können nur starten, wenn sie auf einer Positivliste stehen. Unbekannte Programme sind nicht vertrauenswürdig und dürfen nicht starten.

Systemsicherheit am ITMZ

Wie konfiguriere ich ein sicheres und robustes System?

Drei grundlegende Konfigurationsänderungen

2. **Isolieren** per Firewall:

   Unbekannter ausgehender und eingehender Netzwerkverkehr ist nicht vertrauenswürdig und wird unterbunden.

Systemsicherheit am ITMZ

Wie konfiguriere ich ein sicheres und robustes System?

Drei grundlegende Konfigurationsänderungen

3. **Herabstufen** per Reduzierung der Rechte von administrativen Konten:
   - Standardmäßige Nutzung von Normalbenutzerrechten für administrative Konten
   - Keine automatische Nutzung von administrativen Rechten für administrative Konten

Universität Rostock Traditio et Innovatio

Systemsicherheit am ITMZ

- *Stand der Sicherheit bei aktuellen Windows-Systemen - das Positive, das Negative und das „Hässliche“*

Systemsicherheit am ITMZ

Sicherheit bei aktuellen Windows-Systemen – das Positive

- Keine automatische Nutzung von administrativen Rechten auf Client-Systemen durch UAC
- Reichweite von administrativen Konten auf Client-Systemen auf lokale Zugriffe beschränkt durch LocalAccountTokenFilterPolicy-Registry-Schalter
- Rechtereduzierung beim Zugriff auf das Internet durch Protected Mode des Internet Explorers

Systemsicherheit am ITMZ

Sicherheit bei aktuellen Windows-Systemen – das Positive

- Firewall für eingehenden Verkehr standardmäßig eingeschaltet und eingeschränkt auf notwendige Prozesse
- Reduzierung von offenen Ports durch dutzende Firewall-Blockregeln für aktive Dienste
- Reduzierung von Diensten, die unter dem Systemkonto gestartet werden

Systemsicherheit am ITMZ

Sicherheit bei aktuellen Windows-Systemen – das Positive

- Windows Updates standardmäßig eingeschaltet
- Malware-Scanner Windows Defender standardmäßig aktiv
- Kostenloser Virenscanner Microsoft Security Essentials per Web-Download verfügbar

Systemsicherheit am ITMZ

Sicherheit bei aktuellen Windows-Systemen – das Negative

- Automatische Nutzung von administrativen Rechten auf Server-Systemen
- Beliebige Software ist startbar
- Beliebiger ausgehender Netzwerkverkehr ist erlaubt
- Uneingeschränkte Reichweite von administrativen Active Directory-Konten

Systemsicherheit am ITMZ

Sicherheit bei aktuellen Windows-Systemen – das „Hässliche“

- Während des Setups generiertes Nutzerkonto ist administratives Konto
- Von Microsoft gepflegte Whitelist für UAC-Zustimmungsabfrage (ab Windows 7)
- Uneingeschränkte Reichweite der standardmäßig geöffneten Firewallports

Systemsicherheit am ITMZ

Sicherheit einer Standard-Windows-Installation in Bezug auf die Grundannahme:

Je eingeschränkter Programmvielfalt, Netzwerkverkehr und Zugriffsrechte, je mehr Sicherheit.

- Beliebige Software ist ausführbar.
- Beliebiger ausgehender Netzwerkverkehr ist erlaubt. Beliebiger eingehender Netzwerkverkehr auf alle standardmäßig geöffneten Ports ist erlaubt.
- Administrative Schreibzugriffe sind auf Servern automatisch ohne Zustimmungsabfrage erlaubt und uneingeschränkte Reichweite administrativer AD-Konten

Universität Rostock

Traditio et Innovatio

Systemsicherheit am ITMZ

- *Immunisierung von Windows durch Anwendung von Standard-Windows-Funktionalitäten*

Systemsicherheit am ITMZ

Immunisierung durch Anwendung von Standard-Windows-Funktionalitäten

1. Software Whitelisting (verfügbar ab Windows XP) - Einschränkung der Ausführbarkeit von Programmen mittels Software Whitelisting.

   Grundprinzip: *Verbiete das Ausführen von beliebigen Programmen und erlaube nur noch das Ausführen von autorisierten Programmen.*

2. Firewall (verfügbar ab Windows 2000) - Isolierung des Systems vom Internet mittels Windows Firewall und/oder IPsec-Paketfilter.

Systemsicherheit am ITMZ

Immunisierung durch Anwendung von Standard-Windows-Funktionalitäten

3. UAC (verfügbar ab Windows Vista) - striktes Herabstufen jedes administrativen Tokens mittels Mandatory Integrity Control (MIC) und Deaktivierung automatischer Rechtegewährung für administrative Konten.

4. Zwei-Faktor-Authentifizierung (verfügbar ab Windows 2000) - durch Einschränkung der Reichweite eines Kontos mittels Windows-Nutzerverwaltung und Windows-Firewall-Regeln.

Systemsicherheit am ITMZ

Immunisierung durch Anwendung von Standard-Windows-Funktionalitäten

4. Zwei-Faktor-Authentifizierung durch

   a) Einschränken der erlaubten Systeme an denen sich das zu schützende Konto anmelden darf mittels workstations-Schalter net user-Befehls
   b) Einschränken des Zugriffs auf den Remote Desktop-Port 3389 per IP-ACL der Windows Firewall und/oder IPsec.
   c) Deaktivieren aller betriebssystemfremden Add-Ons, welche eine interaktive Anmeldung erlauben, wie z.B. sshd, VNC usw.

   Authentifizierungsvoraussetzung:
   1. Faktor: Administrator-Passwort (Wissen)
   2. Faktor: Zugang zu den zugelassenen Systemen (Besitz).

Systemsicherheit am ITMZ

Auswirkungen der Konfiguration

- Deaktivierung aller Angriffsvektoren, welche den Start von unerwünschter Software für Systemangriffe voraussetzen.
- Angriffe können nur noch mit zugelassener vertrauenswürdiger Software erfolgen.

Systemsicherheit am ITMZ

Auswirkungen der Konfiguration

- Einschränkung der Reichweite administrativer Konten auf bestimmte Systeme durch Aktivierung von Zwei-Faktor-Authentifizierung für diese Konten

- Alle Angriffsvektoren die Netzwerkverkehr voraussetzen, werden durch die Isolierung des Systems vom Internet stark eingeschränkt.

  Firewall-Regeln isolieren das System vom nicht vertrauenswürdigen Internet und gewähren nur zugelassenen IP-Adressen Netzwerkzugriff.

  Dies betrifft sowohl eingehenden als auch ausgehenden Netzwerkverkehr.

Systemsicherheit am ITMZ

Wovor schützt die Konfiguration?

- Systemweite Veränderung des Systems durch unerlaubte Programme (Installation von Malware, Löschen von Daten usw.)
- Löschen, Veränderung oder Diebstahl von Nutzerdaten durch unerlaubte Programme

Systemsicherheit am ITMZ

Wovor schützt die Konfiguration nicht?

- *Vor Angriffen auf oder durch zugelassene Software wie z.B. Browsern, Mailprogrammen, Viewern, Textverarbeitungen usw.*
- *Vor 0-Day-Exploits, die Fehler in zugelassenen Anwendungen oder im Betriebssystem ausnutzen, um mit vorhandener und zugelassener Software unerwünschte Aktionen durchzuführen.*
- *Vor dem Start von beliebiger Software und beliebigen Skript-Dateien durch das built-in Benutzerkonto System.*

Universität Rostock

Traditio et Innovatio

Systemsicherheit am ITMZ

- *Konfigurations-Toolkits für Windows – Hilfsmittel für Administratoren von selbstverwalteten Windows-Systemen*

Systemsicherheit am ITMZ

Konfigurations-Toolkits für Windows:

Motivation

- Laut den Webserverstatistiken für www.uni-rostock.de weit über 90 Prozent aller Clients unter Betriebssystem Windows, s.

  https://teamsrv.uni-rostock.de/sites/urz/systems/www/Public/webstatistics.htm

  (Daten für 02/2011: Windows 96,4 %, MAC OS X 1,5 %, Linux 1,3 %)

- Daher sinnvoll, sich verstärkt um die Absicherung von Windows zu kümmern

Systemsicherheit am ITMZ

Konfigurations-Toolkits für Windows:

Grundidee

- Nutzung von Windows-Bordfunktionalitäten, um Windows-Systeme robust gegenüber entfernt oder lokal interaktiv ausgelösten Angriffen und administrativen Fehlern zu machen.

Zielgruppe

- Administratoren selbstverwalteter Windows-Systeme

Systemsicherheit am ITMZ

Konfigurations-Toolkits für Windows:

Umsetzung von Sicherheitsregeln durch Skript-Toolkits

- Webdokumentation: Kurzanleitung zur Nutzung der Toolkits als Einstieg in Nutzung und in ausführliche Dokumentation
- Zwei Konfigurationen für unterschiedliche Zielumgebungen
  - Minimalabsicherung - empfohlen für alle Clients
    - Schnellabsicherung - QuickWinSec.bat
  - Vollständiger Schutz – empfohlen für Server
    - Best Practice Windows Sicherheitskonfiguration – WinConfig-Toolkit
      - » Applocker-Toolkit - SRP-Skripte
      - » Firewall-Toolkit - FW-Skripte
      - » Integritäts-Toolkit - FC-Skripte

Systemsicherheit am ITMZ

Konfigurations-Toolkits für Windows:
Vorteile der Konfiguration

- Windows-Systeme funktionieren langfristig zuverlässiger und vorhersehbarer, verglichen mit der Standardkonfigurationen.
- Windows-Patches können nach dem Rhythmus der jeweiligen Organisation eingespielt werden und müssen nicht immer sofort installiert und aktiviert werden.
- Die Reichweite von administrativen Konten ist auf vertrauenswürdige IP-Addressen beschränkt, so dass möglichst lange und komplexe Passworter durch kürzere praktikablere Passwörter ersetzt werden können.

Systemsicherheit am ITMZ

Konfigurations-Toolkits für Windows:
Vorteile der Konfiguration

- Die PC-Hardware kann wieder vorrangig für ihre ursprünglichen Aufgabe genutzt werden: erwünschte Software auszuführen.

  Software Blacklisting ist nur noch notwendig, wenn neue ungeprüfte Software ausgeführt werden soll.

- Die Akzeptanz von UAC wird durch UAC-Helper erhöht, so dass das Arbeiten als eingeschränkter Administrator unter UAC (administrativer Zugriff nur über Zustimmungsabfrage) selbstverständlicher und das Arbeiten als uneingeschränkter Administrator (wie in alten Windows-Versionen vor Windows Vista und vielen alternativen Betriebssystemen) "unnatürlich" erscheint.

Systemsicherheit am ITMZ

Konfigurations-Toolkits für Windows:
Nachteile der Konfiguration

- Für die Installation von neuer Software einschließlich von Windows Updates muss das Software Whitelisting rekonfiguriert werden, da sich die neue Software noch nicht auf der Software Whitelist befindet.
- Diverse Netzwerkprotolle, welche sich nicht über einen lokalen Proxy-Server lenken lassen, z.B. Multimediastreaming-Protokolle, erfordern eine Anpassung der Isolierung vom Internet durch die Windows Firewall und/oder den IPSec-Filter.
- Die strikte Durchsetzung von UAC verringert die Produktivität durch mehr GUI-Arbeit (Bejahen der Zustimmungsabfragen), dies wird aber deutlich kompensiert durch den Mehrgewinn an Sicherheit und nicht zuletzt auch durch den erhöhten Schutz vor Fehlern, z.B. versehentliches Löschen von Daten.

Universität Rostock

Traditio et Innovatio

Systemsicherheit am ITMZ

- *Microsoft Security Essentials 2.0*

Systemsicherheit am ITMZ

Microsoft Security Essentails 2.0

Vorteile gegenüber Sophos Anti-Virus

- Kostenlos
- Konfigurationsarm
- Ressourcenschonend

Nachteile gegenüber Sophos Anti-Virus

- Windows-only