IPv6 Security Briefing (half day)

Understanding the new security issues introduced by IPv6 and the actions you should take.

About this Briefing

IPv6 is now used by default by most operating systems and many network devices. It is widely available and increasingly deployed. In some parts of the world and in some organisations, IPv6 is mandatory.

Even though you may not have deployed IPv6 in your network yet, you still need to secure your network against abuse through IPv6 protocols and services using IPv6.

Modern network operating systems, including Windows Vista, Windows 7, Windows Server 2008, Linux and Unix will use IPv6 in preference to IPv4 and have IPv6 turned on by default.

You need to ensure that your network is IPv6 secure and that you are ready for any future implementation of IPv6.

Relevant Platforms:

This briefing applies to all platforms, including:

- **Cisco IOS**
- **Linux (all distributions)**
- **Unix**
  - **AIX**
  - **HP-UX**
  - **Solaris**
- **FreeBSD**
- **Windows**
  - **Windows 2000**
  - **Windows XP**
  - **Windows Server 2003**
  - **Windows Vista**
  - **Windows 7**
  - **Windows Server 2008 R2**

You will learn

- The current status of IPv6
- The security features of IPv6
- The security risks introduced by IPv6
- How IPv6 security differs from IPv4 security
- The risks associated with IPv6 transition mechanisms.
- How to mitigate the security risks associated with IPv6.
- How to configure IPv6 firewalls.
- IPv6 security best practice.

.

Briefing Contents

Review of IPv6

- Comparison of IPv6 and IPv4
- What is IPv6?
- Why is IPv6 required?
- Address Space
- Is there an address shortage?
- IPv6 improvements over IPv4
- New features in IPv6
- The benefits of IPv6
- Motivations to implement IPv6
- IPv6 status summary
- Timescale predictions

IPv6 Security Features

- Security features in IPv6
- IPv6 IPSec
- Privacy Addresses
- Cryptographically Generated Addresses (CGA)
- SEcure Neighbor Discovery (SEND)
- Mobile IPv6 security
- Dynamic routing security
- Examples of IPv6 security

IPv6 Security Threats

- Summary of IPv6 threats
- Comparison of IPv6 with IPv4 threats
- Threats common to IPv4 and IPv6
- IPv6 specific security threats
- End-to-end transparency
- Scanning in IPv6
- IPv6 extension header threats
- IPv6 router header abuse
- IPv6 fragmentation threats
- ICMPv6 threats
- Neighbor discovery threats
- ND threat examples
- SEcure Neighbor Discovery (SEND)
- Cryptographically Generated Addresses (CGA)
- SEND and CGA
- Mitigating ICMPv6 threats

IPv6 Transition Security Threats

- IPv6 transition mechanisms threats
- Transition mechanisms
- Transition security problems
- Dual stack threats
- Mitigating dual stack threats
- Tunnelling threats
- 6to4 threats
- Mitigating 6to4 threats
- ISATAP threats
- Mitigating ISATAP threats
- Teredo threats
- Mitigating Teredo threats
- Other mechanisms
- IPv6 DNS threats
- Transition security best practice

IPv6 Firewalls

- Configuring IPv6 firewalls
- IPv6 firewall filtering rules
- Filtering ICMPv6
- IPv6 extension headers
- Implementing IPv6 Ingress filtering
- Assigned IPv6 addresses
- Status of IPv6 firewalls
- Deploying IPv6 firewalls

IPv6 Deployment Risks

- IPv6 pilots
- IPv6 DNS server
- Addressing schemes
- Deploying ICMPv6
- End-to-end transparency
- IPSec transport mode
- Reduced functionality
- Operational issues
- ND proxies
- Training

IPv6 Security Best Practice

- Creating an IPv6 security policy
- Summary of IPv6 security best practice

Who Should Attend

This course is ideal for IT security experts, network administrators, network support personnel, network designers, networking consultants, IT managers and IT directors.

The course assumes a knowledge of general networking concepts.

The Speakers

Erion's speakers are practising IPv6 consultants with extensive experience of IPv6.

Further information can be found at:
www.ipv6training.com
www.ipv6consultancy.com
www.erion.co.uk

Company Registration: 3521142
VAT Number: 698 3633 78