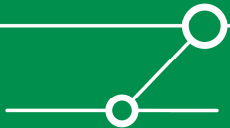


Routing Protocol Security

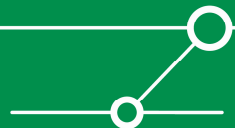
Stand der Technik – eine
exemplarische Risiko Analyse



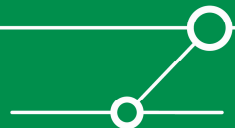
Ihr Referent: Dror-John Röcher



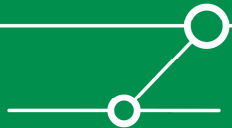
- **Jahrgang 1973**
- **1996 – 2004: freiberuflich tätig als Referent & Berater mit Schwerpunkten “Enterprise Networking” & “Network Security”**
- **Seit 2004: Senior Security Consultant & Gesellschafter, ERNW GmbH**
- **Ausgewählte Vorträge/Publicationen:**
 - Security Patchmanagement, IIR Security Forum, 2005
 - Blackberry Security & Mobile Security, itsecurity, 2006
 - OSPF Security: Vortrag & Tool-Release, IT-Underground, Prag, 2007
 - NAC@ACK – Hacking the Cisco NAC Framework, Vortrag & Tool-Release, Blackhat 2007, Amsterdam
- **Kontaktdaten:**
 - Email: droecher@ernw.de
 - Mobil: 0173-6745905



- **Einführung**
- **Routing-Protokolle: Bedrohungen & Schwachstellen**
 - Allgemein
 - Exemplarisch für OSPF
 - Exemplarisch für HSRP
- **Zusammenfassung**

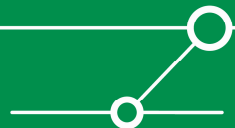


Einführung

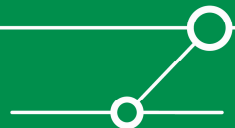


- **Alles, was benötigt wird um IP-Pakete von einem Absender zu einem Empfänger zu transportieren:**
 - Kabel
 - Switche
 - Router
 - Protokolle:
 - OSI-Layer2-Protokolle (STP, ARP, etc)
 - OSI-Layer3-Protokolle (IP, ICMP, OSPF, IS-IS, etc)

- **Infrastruktur-Security betrachtet alle Parameter – im Vortrag werden nur Protokolle auf OSI-Layer3 betrachtet.**



- **Die (Netzwerk)-Infrastruktur bildet die gemeinsame Grundlage für Dienste & Applikationen:**
 - Mail, Internet
 - SAP, Oracle
 - ActiveDirectory, LDAP
 - Datei- und Druckdienste
 - etc.
- **Auf einer nicht-vertrauenswürdigen Infrastruktur können keine vertrauenswürdigen Dienste angeboten oder betrieben werden.**
- **Ergo: Vertrauenswürdigkeit (Sicherheit?) der Infrastruktur sollte hohe Priorität haben.**



■ Verfügbarkeit

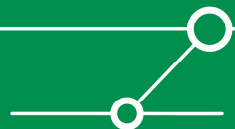
- Die Infrastruktur sollte die gleiche Verfügbarkeit wie die Applikation mit der höchsten Verfügbarkeit haben.

■ Integrität

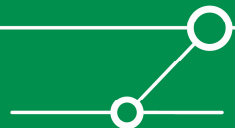
- Infrastrukturprotokolle bestimmen, auf welchem Weg Informationen im Netzwerk transportiert werden. Die Integrität dieser Protokolle schützt somit die Vertraulichkeit und Integrität der transportierten Informationen indem der unautorisierte Zugriff auf die Daten während des Transports unterbunden wird.

■ Authentizität

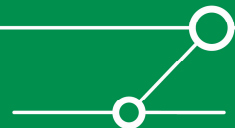
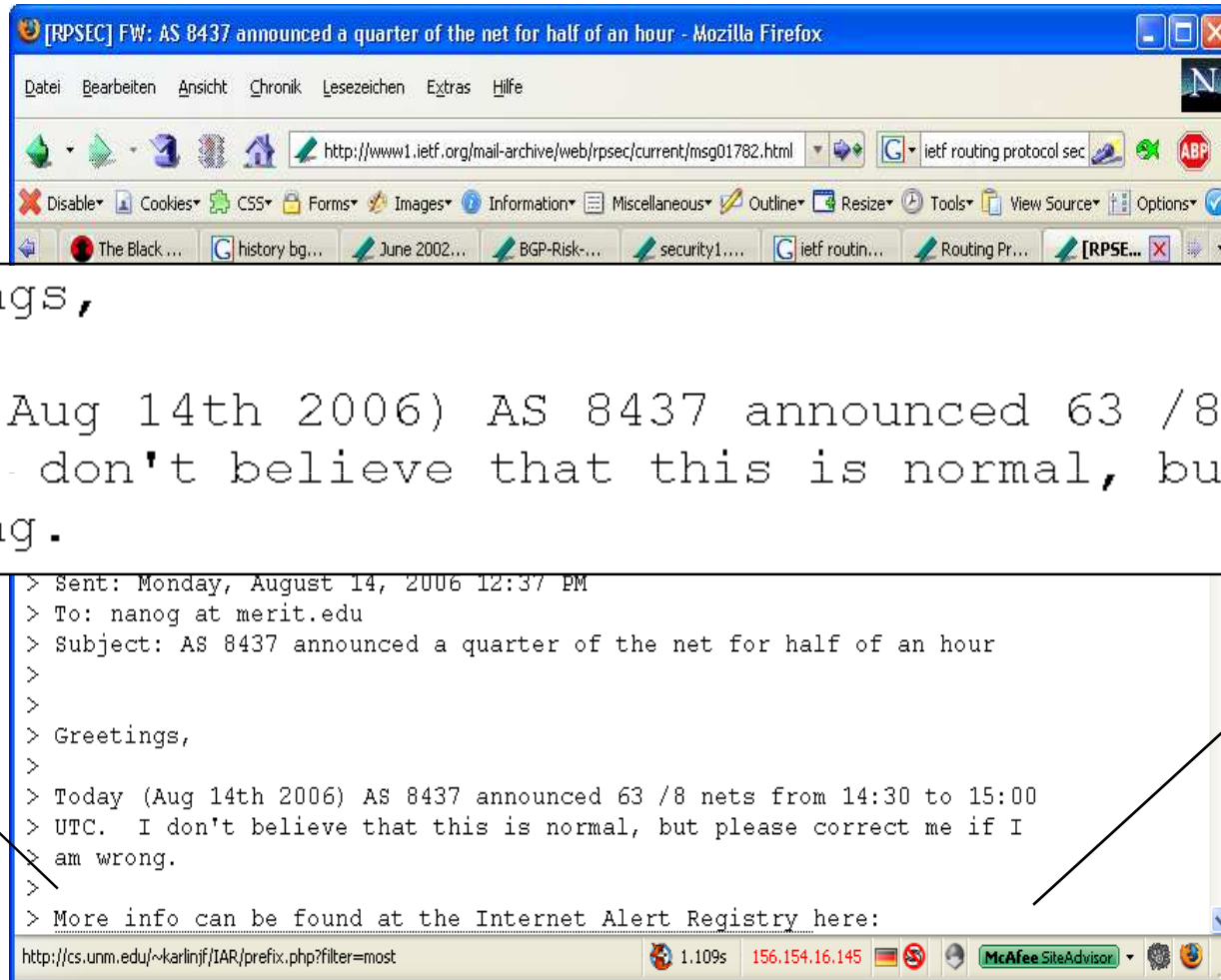
- Das Einbringen nicht authentifizierter (und nicht autorisierter) Infrastruktur-Devices gefährdet die Verfügbarkeit der Infrastruktur und die Vertraulichkeit und Integrität der transportierten Daten.



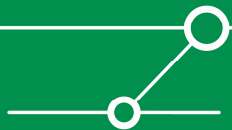
- **Infrastruktur-Sicherheit erhält heute weniger Aufmerksamkeit als noch vor einigen Jahren.**
- **Security wird von Trends getrieben:**
 - “Web-App-Security” als Trend
 - “Client-Security” als Trend
 - “Mobile Security” als Trend
 - “Compliance” als Trend
- **Und hinzu kommt:**
 - Netzwerk-Infrastruktur wird als “Commodity” betrachtet
 - ‘Admin-Schmerzen’: Zeit, Know-How, Budget
 - Oft outgesourct – mit fragwürdigen Implikationen bzgl. der Security
 - Und ausserdem: “Es läuft doch...”



Zum Thema „Es läuft doch“... menschliches Versagen als Ursache

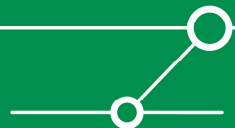


Routing Protokolle: Bedrohungen & Schwachstellen



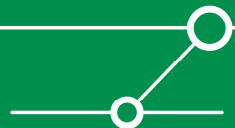
- **BGP** hält das Internet am Leben (neben DNS & Koffein).
- **OSFP & IS-IS & EIGRP** wird innerhalb von Unternehmensnetzwerken eingesetzt.
- **RIP** ist [zum Glück] so gut wie ‚tot‘.

- **Zusätzlich noch einige Routing-nahe Protokolle:**
 - HSRP: Router Redundanz
 - VRRP: Router Redundanz
 - GLBP: Router Load-Balancing



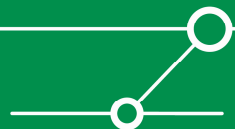
■ Manipulation der Routing-Information mit folgenden Konsequenzen:

- Beeinträchtigung der Verfügbarkeit der Infrastruktur bis hin zum Denial of Service.
- Verlust der Vertraulichkeit der transportierten Daten (Stichwort “sniffing”).
- Verlust der Integrität der transportierten Daten (Stichwort “Man in the Middle”).



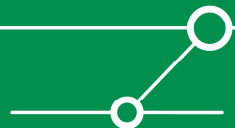
Bedrohungen formal – gegen die Protokolle

- **TP1: Schlecht designte Protokolle können zum Verlust von Vertraulichkeit/Integrität/Verfügbarkeit führen.**
- **TP2: Implementation können BufferOverflows und ähnliche Fehler enthalten.**
- **TP3: Komplexität der Protokolle können zu Fehlkonfigurationen führen.**



Bedrohungen formal – gegen die Datenverbindungen

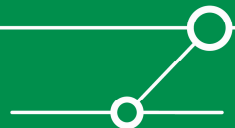
- ***TD1: Sniffing/Mitlesen von Daten (Verlust der Vertraulichkeit)***
- ***TD2: Datenmodifikation (Verlust der Integrität)***
- **Denial-of-Service (Verlust der Verfügbarkeit):**
 - TD3: - durch einen Angriff***
 - TD4: - durch eine Fehlkonfiguration/Fehleinschätzung (ungenügende Ressourcen/Kapazitäten, etc.)***



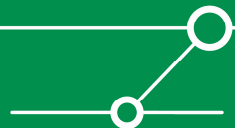
Bedrohungen formal – gegen die Infrastruktur-Komponenten

- **TK1: Systemkompromittierung**
 - ⇒ Sniffing/Mitlesen von Daten
 - ⇒ Umleitung von Datenverbindungen
 - ⇒ Missbrauch der Ressourcen
 - ⇒ Modifikation der Konfiguration

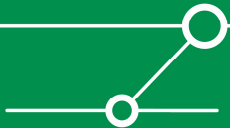
- **TK2: Denial-of-Service (Verlust der Verfügbarkeit)**
 - Angriff gegen die Komponenten selbst



- **Schwachstellen auf Protokollebene**
 - SP1: “designed without security in mind” (meistens keine Authentifizierung, keine Verschlüsselung, etc. bzw. Nachträglich ‘on top’ implementiert).
 - SP2: Schlechte Kennwörter, unterliegen nicht der Passwort-Policy (Bsp.: OSPF-Authentifizierungs-Kennwort wird nicht geändert).
- **Schwachstellen auf Datenverbindungsebene**
 - SD3: Üblicherweise unverschlüsselt
- **Schwachstellen auf Infrastruktur-Komponenten-Ebene**
 - SK1: Unsicheres Management (SNMP, Telnet, HTTP)
 - SK2: Schlechte Kennwörter (Master-Passwörter, etc.)
 - SK3: Unsichere Default-Konfigurationen
 - SK4: Prinzip der “segregation of duties” (Funktionstrennung) oft verletzt

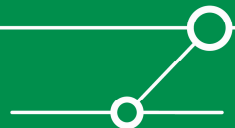


Exempli Gratia: OSPF



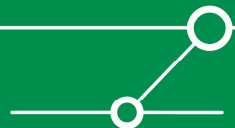
- **Beginn der Entwicklung durch das IETF:
1987**
- **OSPFv2: RFC 1247 (1991)**
- **Aktuelle Version:
OSPFv2: RFC2328 (1998)**

- **Wichtigster Autor:
John Moy (Ascend Communications)**



OSPF Kurzübersicht (1)

- 1) OSPF-Router versenden Hello-Pakete über alle OSPF-Schnittstellen. Falls 2 Router einen gemeinsamen Link teilen und in den Hello-Paketen bestimmte Parameter übereinstimmen, werden die Router zu „Neighbors“**
- 2) Zwischen bestimmten „Neighbors“ werden „Adjacencies“ gebildet, eine Art besonders „guter“ Nachbarschaft.**
- 3) Jeder Router sendet LSAs an alle Adjacencies. Die LSAs beschreiben alle Links des Routers.**
- 4) Jeder Router, der ein LSA von einem Neighbor erhält, trägt die beschriebenen Links in seiner Link State Database ein und sendet eine Kopie der LSA an seine adjacent Neighbors weiter.**

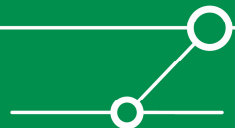


OSPF Kurzübersicht (2)

- 5) **Durch das „flooding“ der LSAs in der gesamten Area hat jeder Router eine identische Topologie-Datenbank, die das gesamte Netzwerk beschreibt.**

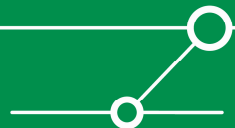
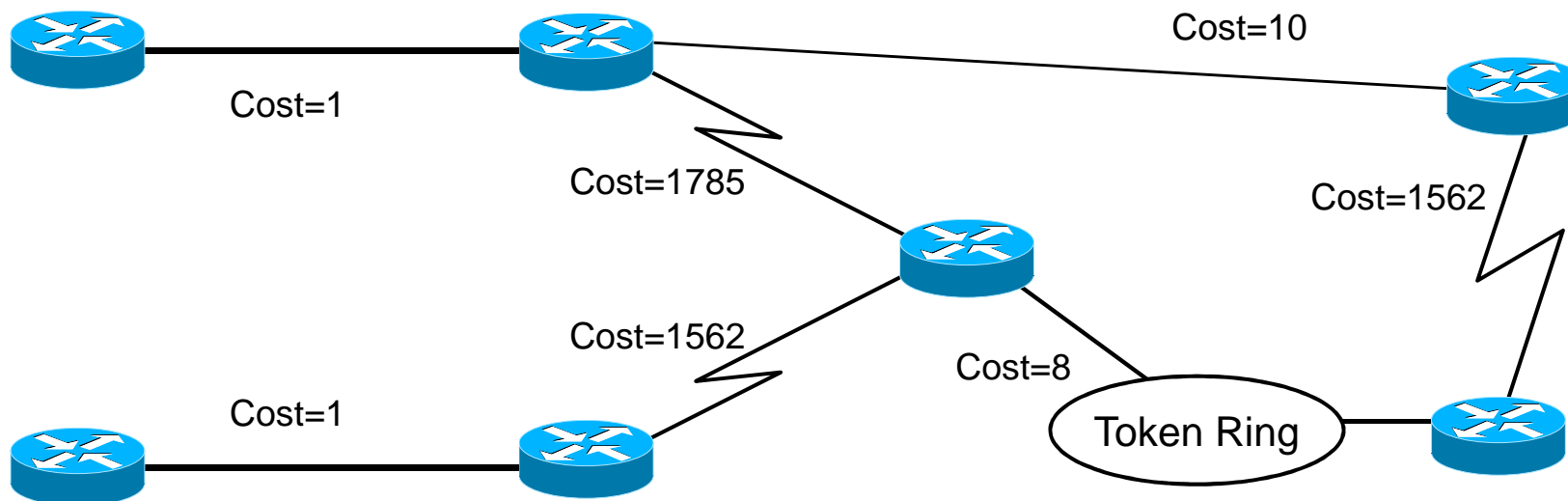
- 6) **Sobald die Datenbanken vollständig und synchron sind, berechnet jeder Router einen Graphen des Netzes, der die „kürzesten“ Wege zu allen Zielen enthält. Dieser Graph ist der „Shortest Path First Tree“**

- 7) **Jeder Router bildet seine Routingtabelle aus dem SPF Tree indem die kürzesten Wege in der Routingtabelle eingetragen werden.**



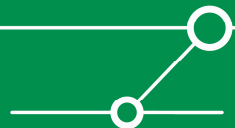
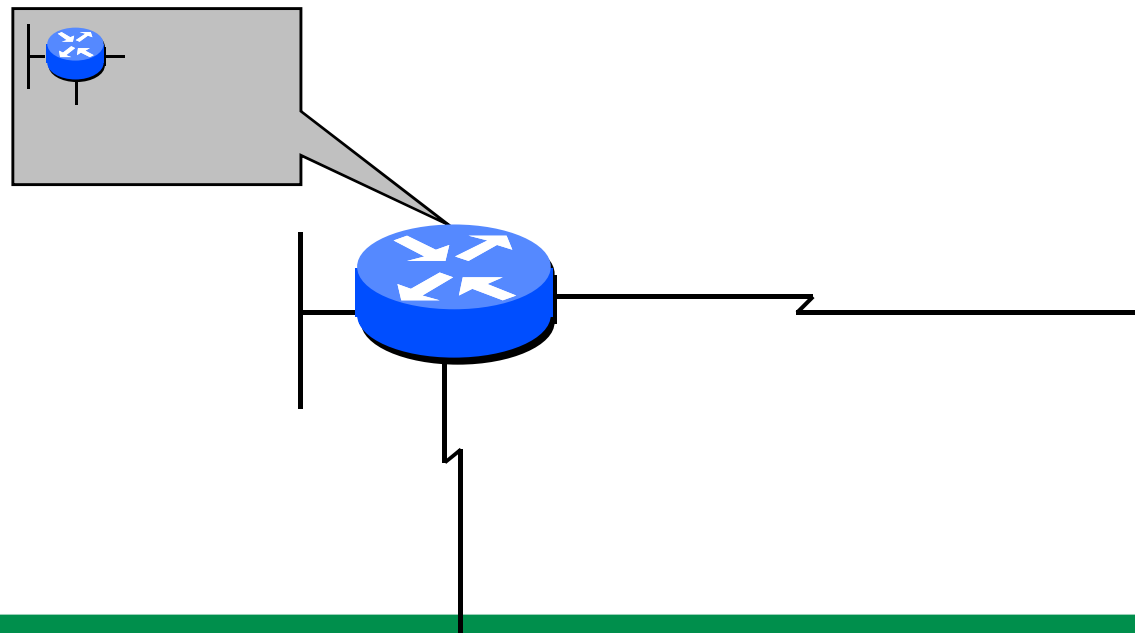
OSPF Metrik

- **Metrik: Kosten**
- **Jeder Link ist mit einem „Kostenwert“ assoziiert**
- **Je niedriger die Kosten, umso besser der Link**
- **Die Kosten zu einem Ziel bestehen aus der Summe der Kosten aller beteiligten Interfaces der Gesamtstrecke**



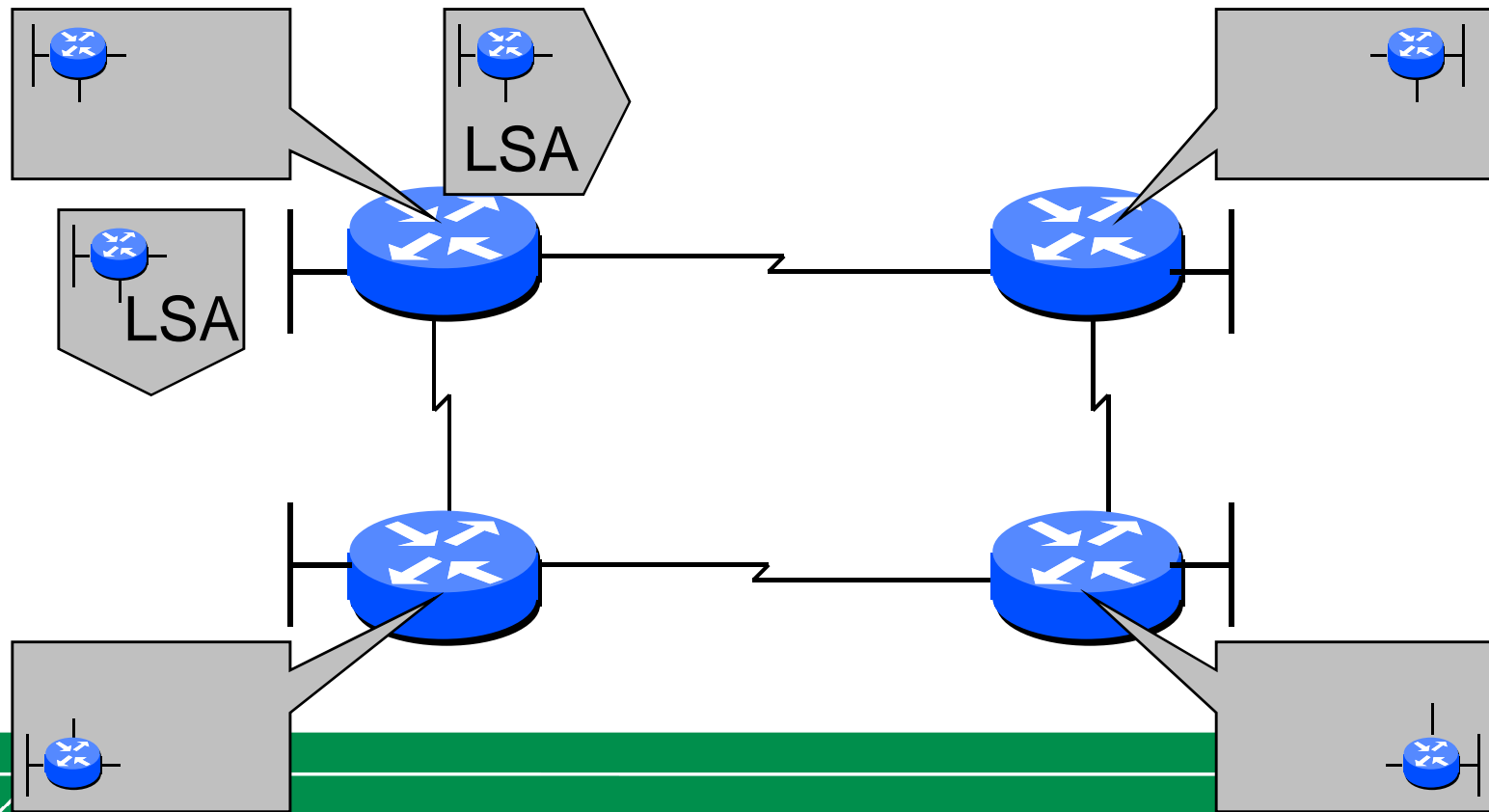
Link State Advertisements

- **Jeder Router erzeugt ein LSA für jeden seiner Links, welches den Link identifiziert, den Zustand des Links beschreibt, die Metrik des Interfaces angibt und die Liste aller bekannten Nachbarn auf dem Link enthält.**



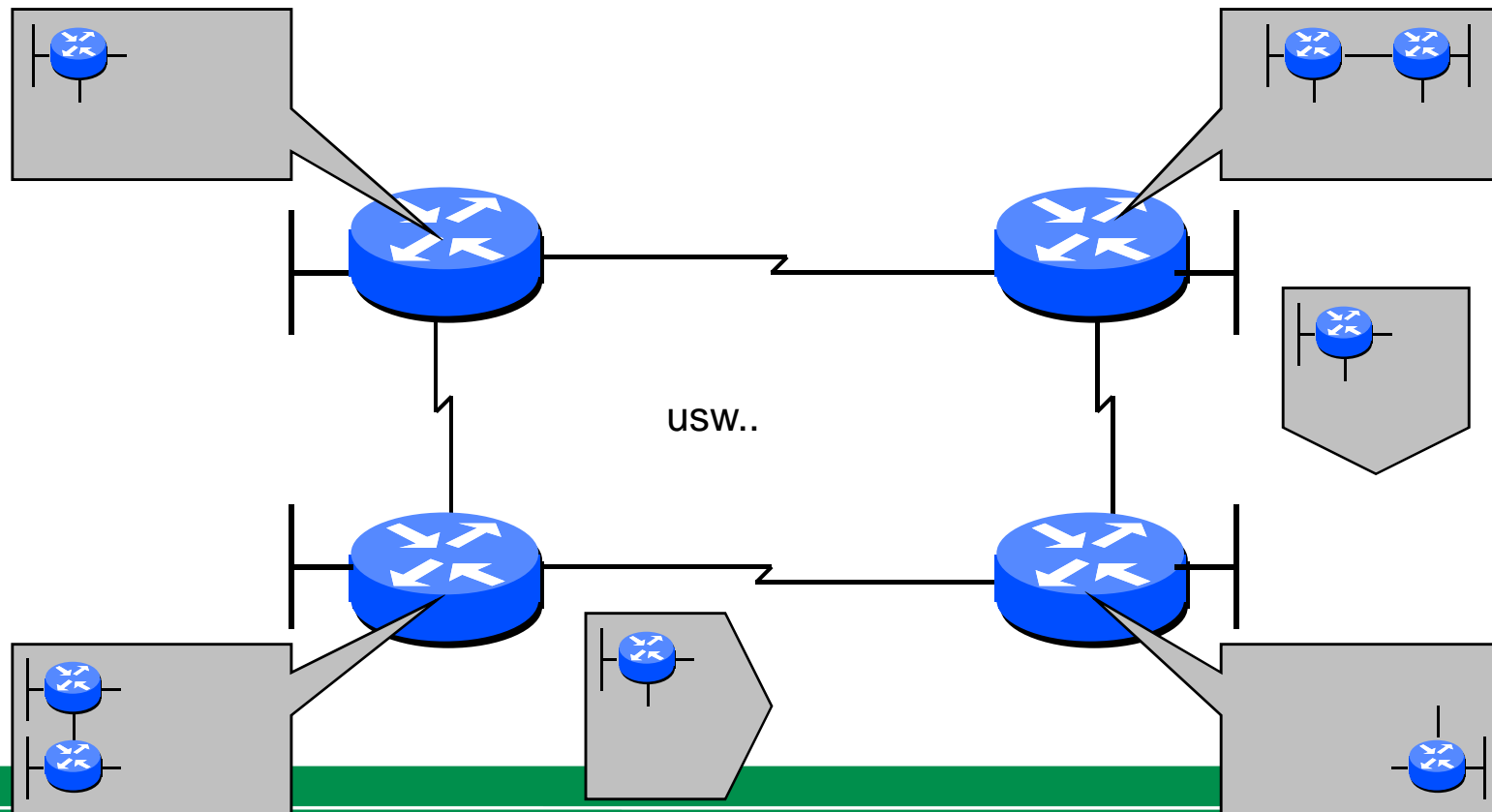
Link State Advertisements

- Die LSAs werden von jedem Router erzeugt und an alle Nachbarn übermittelt.
- Die Nachbarn leiten empfangene LSAs ohne Veränderung an alle ihre Nachbarn weiter (flooding)



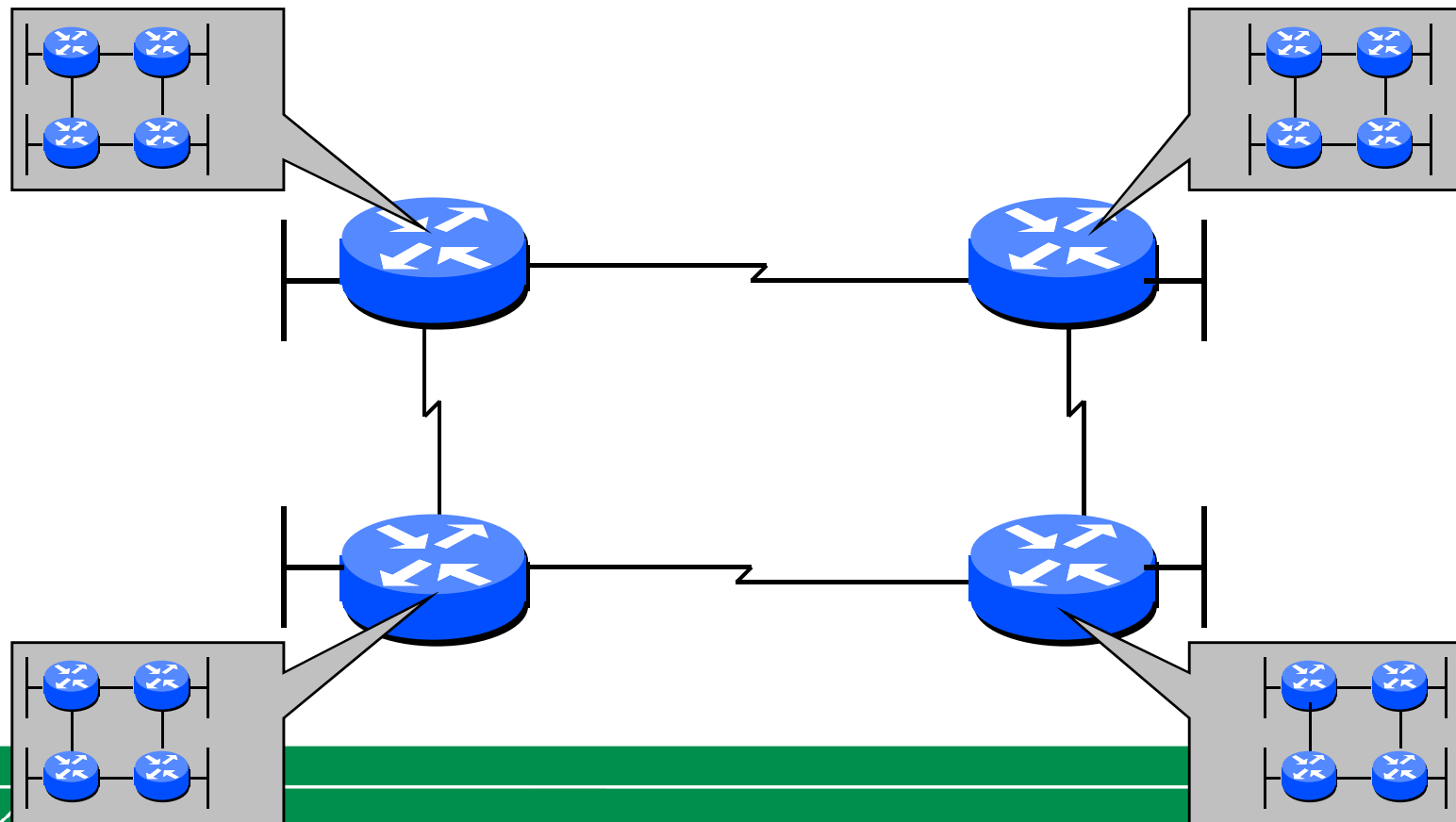
LSA and Flooding

- Jeder Router kopiert den Inhalt der empfangenen LSAs in seine Topologiedatenbank, bevor das LSA an die weiteren Nachbarn übermittelt wird.
- Dadurch hat jeder Router eine komplette Kenntnis des gesamten Netzes



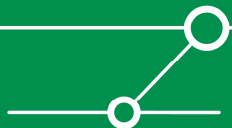
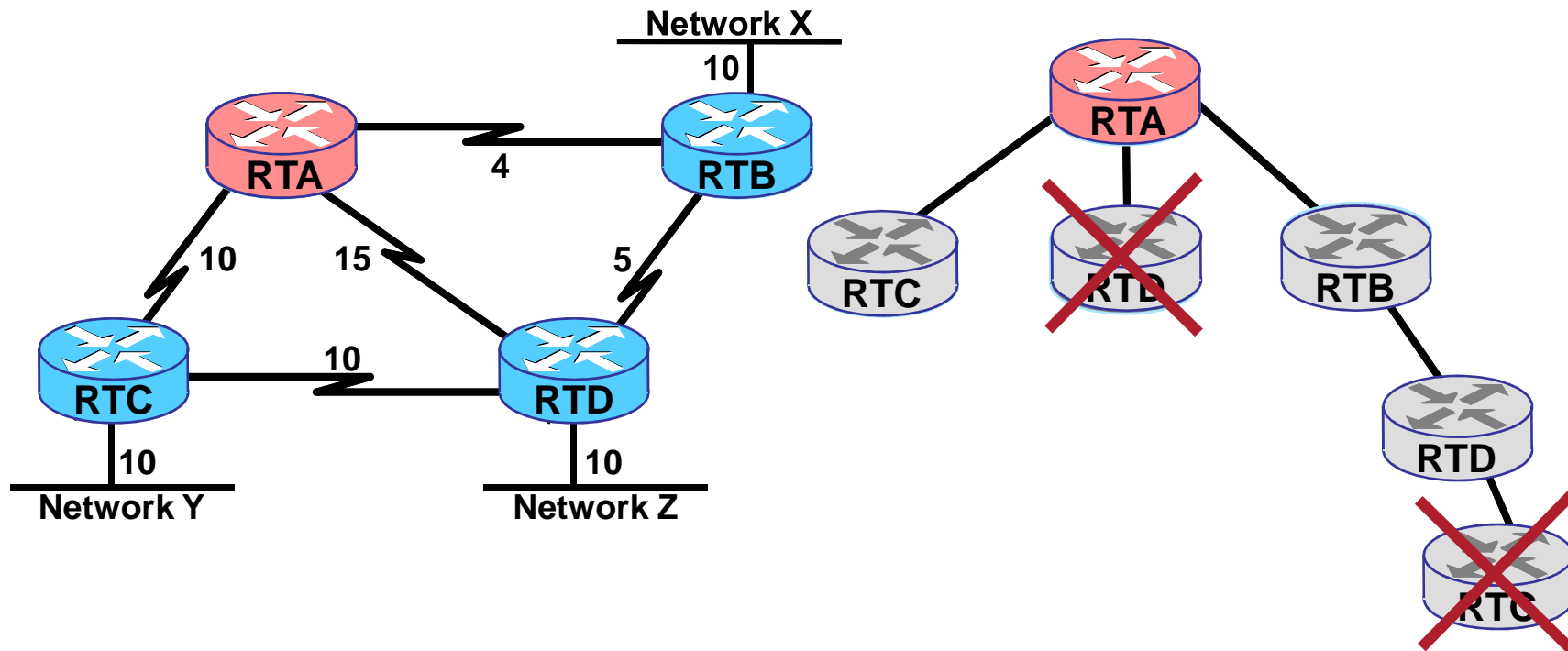
Full Topology

- Die vollständige Topologiedatenbank (link state database) beschreibt einen Graphen des gesamten Netzes



Shortest Path First (SPF)

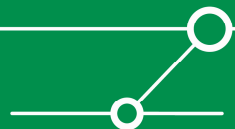
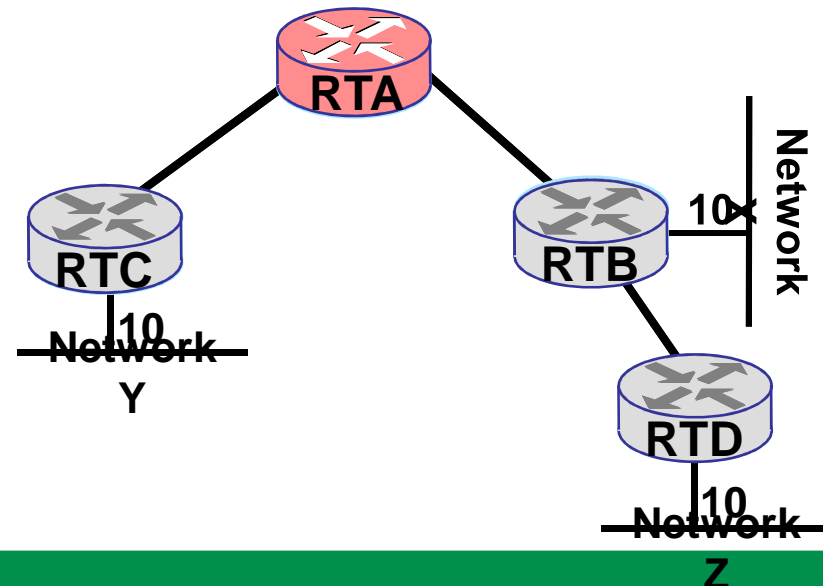
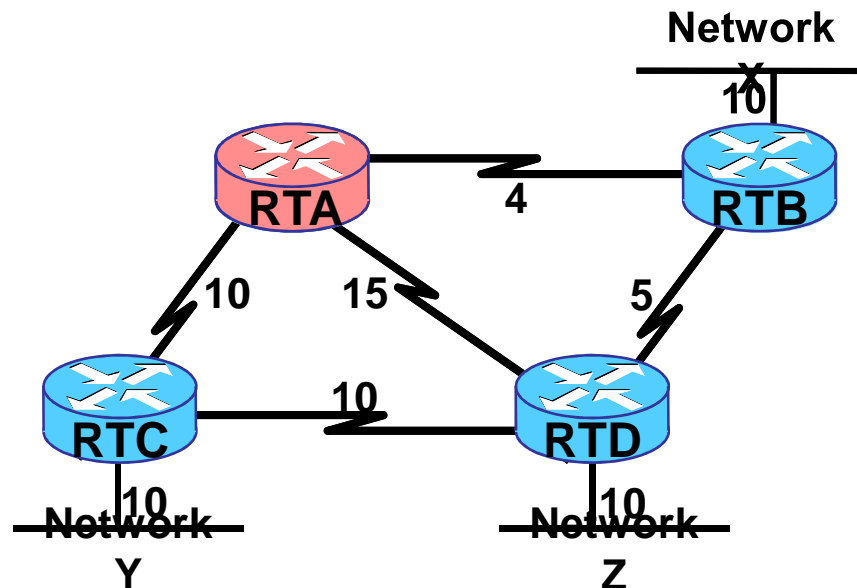
- Aus diesem Graphen können die kürzesten Wege zu allen Zielen im Netz mittels Dijkstras Algorithmus errechnet werden.



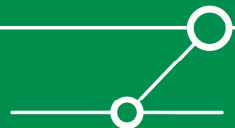
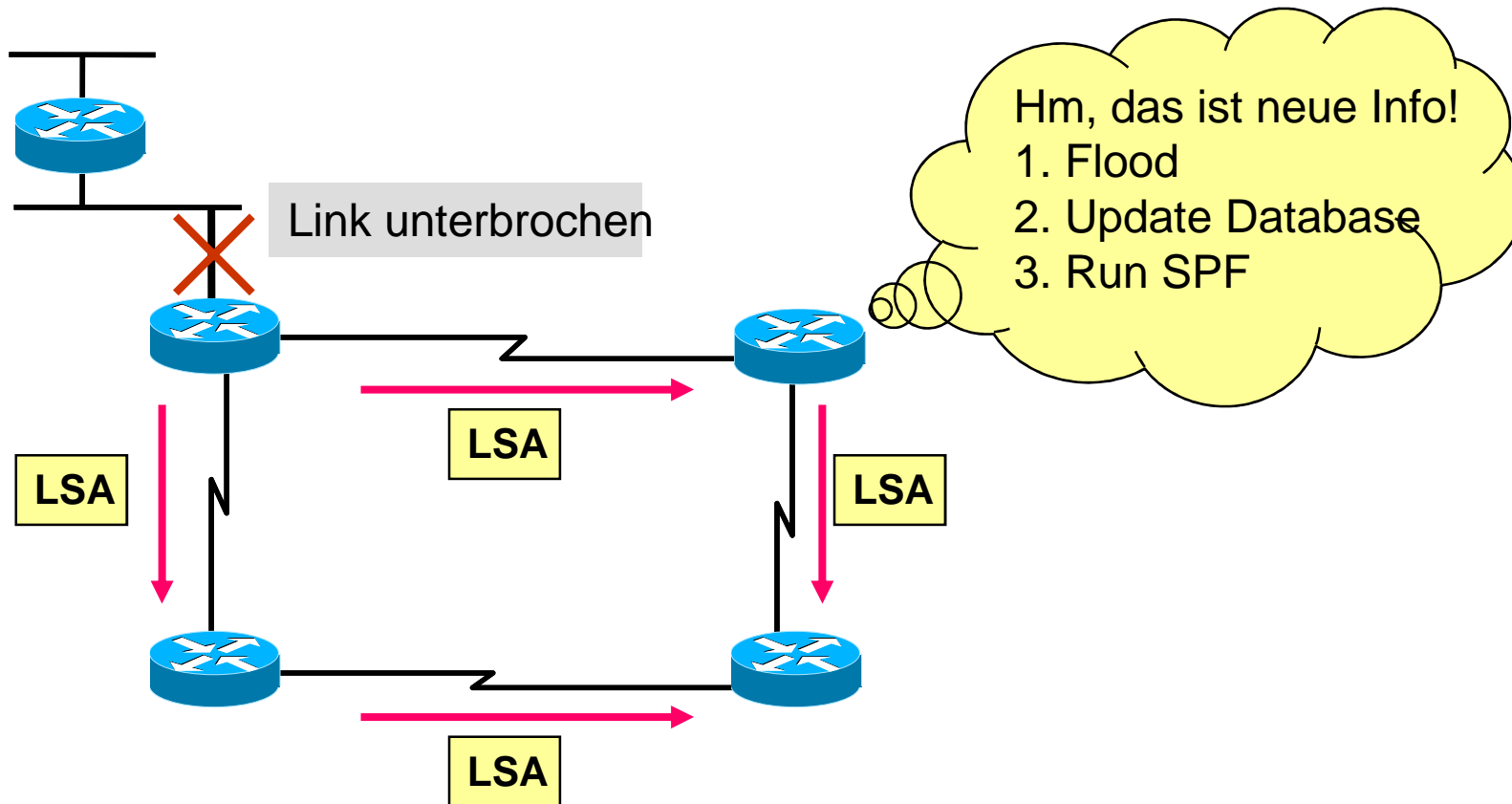
SPF und die Routing-Table

- Diese kürzesten Wege werden dann in die Routingtabelle eingetragen.

Routing Information		
Network	PCost	NextHop
X	4+10	RTB
Y	10+10	RTC
Z	9+10	RTB



Flooding

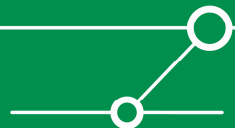


Alle OSPF Pakete können authentifiziert werden um die Sicherheit innerhalb der Routing Domäne zu erhöhen.

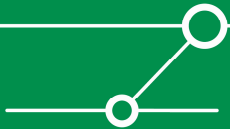
Per default wird keine Authentifizierung benutzt (Null Authentication).

Zur Wahl stehen:

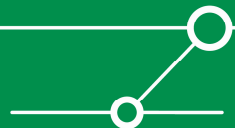
- 1. Simple password authentication (Passwort steht im Klartext in jedem Paket)**
- 2. Message Digest authentication (md5-gesicherte Passwörter in jedem Paket)**



Threats & Vulnerabilities



- **Angriffe gegen OSPF sind rein akademische Gedankenspiele.**
- **Der eingebaute “Fight-Back”-Mechanismus limitiert die Auswirkungen eines Angriffs auf eine sehr kurze Zeitdauer.**
- **Es gibt (öffentlich) kein “Tool” um OSPF anzugreifen.**
 - Proof-of-Concept-Tool (OSPF-Attack-Shell) seit März 2007 auf www.ernw.de frei verfügbar ;-)



- **Angriffe von ausserhalb des OSPF-Netzwerkes**

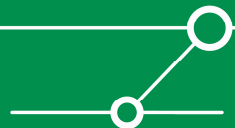
- Voraussetzung: Der Angreifer kann OSPF-Pakete an einen internen OSPF-Router senden. Dies *sollte* nicht möglich sein.

Heutiger Fokus

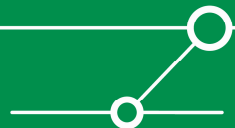
- **Angriffe von innerhalb des OSPF-Netzwerkes**

- **Device Compromise:** Angreifer hat administrative Kontrolle über einen OSPF-Router.
- **Link Compromise:** Angreifer hat Verbindung mit einem Netzwerk-Segment, auf welchem OSPF aktiv ist.

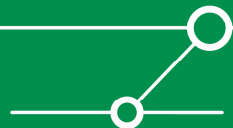
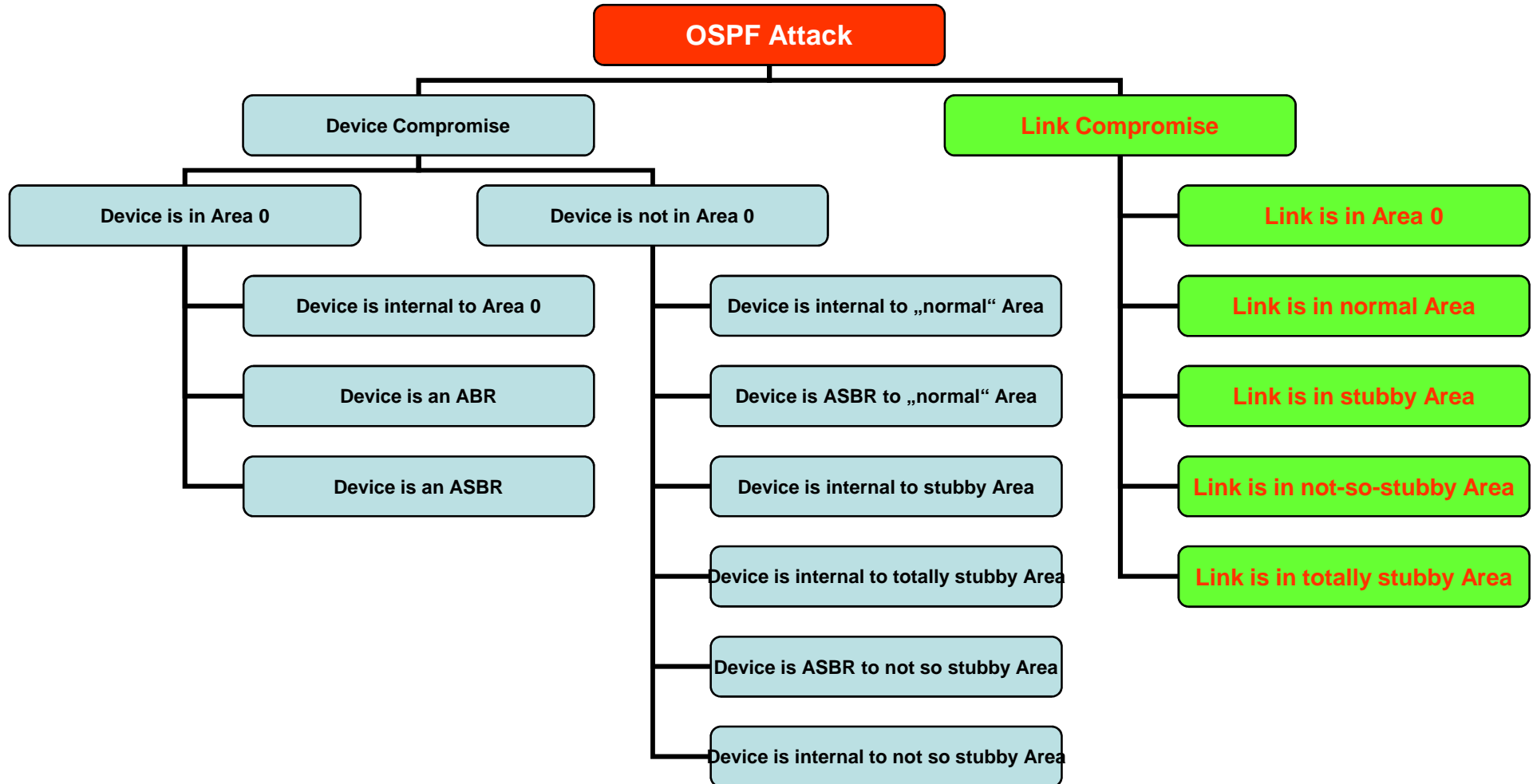
- **Angriffe über „defekte“ Implementationen: BufferOverflow in OSPF-Software etc.**



- **OSPF unterscheidet verschiedene Arten von Links:**
 - Link is in Area 0
 - Link is not in Area 0
 - Link is in „normal“ Area
 - Link is in „stubby“ Area
 - Link is in „not so stubby“ Area
 - Link it in „totally stubby“ Area

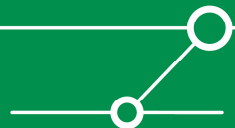


Der ‚Attack-Tree‘



Bedrohungen durch Device-Compromise

- **Ohne auf Details einzugehen:**
 - DoS: Dropping of routes
 - DoS: (Partial) Disabling of OSPF
 - DoS: Addition of „bogus“ routes via loopback interfaces (e.g. with /32 mask to have a „longest match“)
 - DoS: Creating Routing loops (which adds congestion besides DoS)
- **All diese Angriffe sind weniger „interessant“, weil jede Konfigurations-Änderung des kompromittierten Geräts zwangsläufig die lokale Routingtabelle des Geräts verändert – und die „interessanten“ Angriffe (jenseits von DoS) genau dies verhindern müssen.**



Threats durch „Link Compromise“

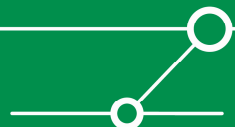
■ Denial of Service:

- **TL1:** Blackhole: Traffic is directed to a router which cannot handle the load.
- **TL2:** Starvation: Traffic is forwarded to a part of the network, that can not deliver it.
- **TL3:** Delay: Traffic is routed via a suboptimal path.
- **TL4:** Loop: Traffic is forwarded along a looping path.
- **TL5:** Partition: Some part of the network believes it is partitioned from the rest.
- **TL6:** Churn: Forwarding on the network changes rapidly, resulting in large variations of data-delivery patterns (impacting congestion control mechanisms).
- **TL7:** Instability: OSPF itself becomes unstable so that global convergence is never achieved.
- **TL8:** Overload: OSPF messages themselves become a significant part of the network traffic.
- **TL9:** Resource Exhaustion: OSPF messages cause exhaustion of router resources (queues, memory, cpu).

Galt bisher als rein theoretischer Natur –
'OSPF-Attack-Shell' machts möglich.

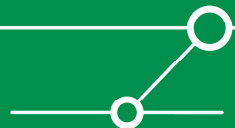
■ Man in the Middle

- **TL10:** Eavesdropping: Carefully crafted insertion of routing information may lead to rerouting through attacker which may put the attacker in the packet-path. These are quite difficult to accomplish. But this is (imho) the most interesting attack scenario.

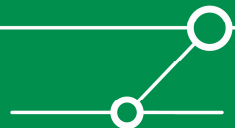
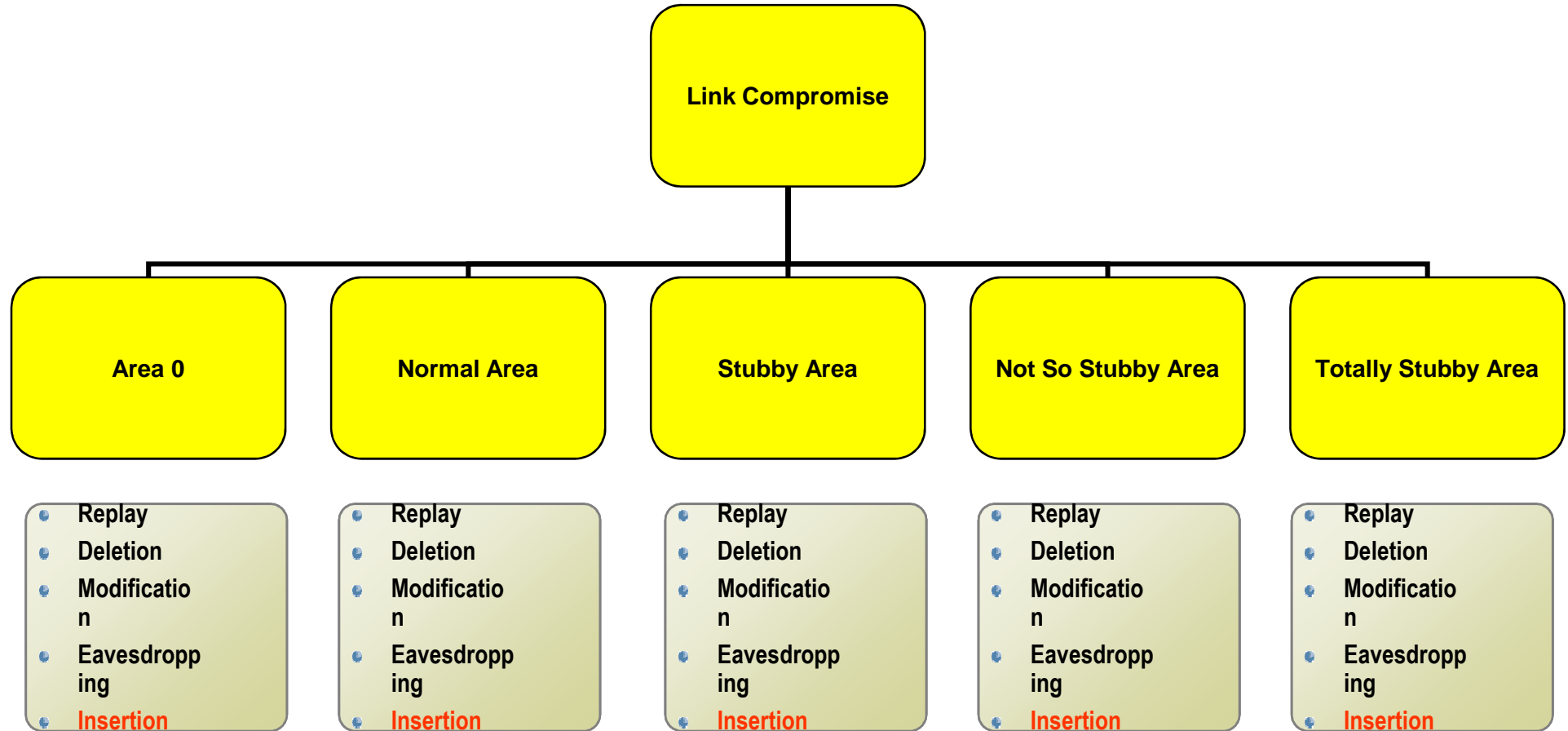


Klassifizierung „Link Compromise“

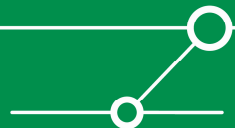
- **Message Replay**
- **Message Insertion**
- **Message Deletion (usually detectable by the sender)**
- **Message Modification**
- **Message Eavesdropping**



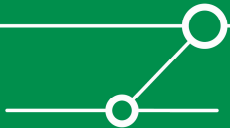
Link Compromise



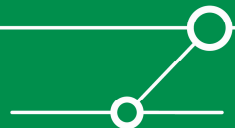
- **VL1:** OSPF Routers on Broadcast, NBMA, PtMP and Virtual Links accept Unicast packets (Section 8.1 in RFC 2328). Therefor many attacks for link-compromise work also „from remote“, as long as the attacker is able to send IP-Protocol-89 packets to a legitimate OSPF router.
- **VL2:** No Authentication
- **VL3:** Plain-Text Authentication
- **VL4:** Usually same key used on all links (if any at all).
- **VL5:** Tools for breaking OSPF-MD5-keys exist (e.g. Cain & Abel)



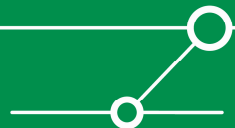
Angriffs-Klassifizierung - **Message Insertion**



- **„Phantom Router“ (nicht existierende Router)**
 - Ein einfaches „hello“-Paket genügt um einen „Phantom-Router“ ins Netz „einzuführen“ – nicht wirklich spannend.
- **Message Spoofing existierender Router**
 - „Hello“ Nachrichten auf Links, an denen der Router nicht angeschlossen ist.
 - „Hello“ Nachrichten auf Links, an denen der Router angeschlossen ist.
 - Gefälschte „LSA“-Pakete – hier greift der „OSPF-Fightback“-Mechanismus, den ein Angreifer ausnutzen kann um einen langanhaltenden DoS zu erzeugen.



- **Hinzufügen eines „echten“ Routers (Angreifer PC wird zum OSPF-Router) um Verkehr umzuleiten/über den Angreifer zu leiten:**
 - In the Backbone Area
 - Inject Type 1,2,3,5 LSAs
 - In a normal Area
 - Inject Type 1,2,3,5 LSAs
 - In a stubby Area
 - Inject Type 1,2,3 LSAs
 - In a totally Stubby Area
 - Inject Type 1,2 LSAs
 - In a NSSA
 - Inject Type 1,2,7 LSAs

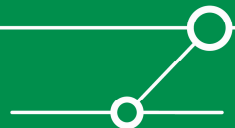


Hinzufügen eines echten Routers...

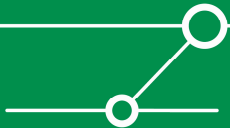


■ Einige Möglichkeiten:

- Hinzufügen eines „neuen“ Netzwerks (e.g. 194.77.14.0/24)
- Hinzufügen eines Netzwerkes, das anderswo innerhalb der OSPF-Domäne existiert.
- Hinzufügen neuer „Areas“ mit „neuen“ oder anderswo vorhandenen Netzwerken.
- ...



„Mitigation Controls“ für OSPF



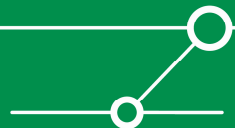
Mitigating attacks on OSPF

■ Präventiv:

- MD5-Authentifizierung mit guten Passwörtern (unterstützen das alle Geräte?)
- Passwörter regelmässig ändern (Widerstand der ‚Netzwerk-Truppe‘ zu erwarten)
- OSPF auf ‚Access-Links‘ (Verbindungen zu Clients/Servern) deaktivieren – am besten per „passive interface“.
- Strenges Ingress-Filtern
 - From outside, of course never ever accept OSPF (ip protocol 89)
 - From access-networks, never ever accept OSPF (ip protocol 89)
 - Multicast Filtering (224.0.0.5 & 224.0.0.6) may come in handy, too.

■ Detektiv:

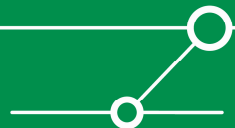
- Monitoring der OSPF „neighbor changes“ (unerwartete neue OSPF-Nachbarn sind ein Hinweis auf unerwünschte Aktivitäten)
- Monitoring der Routing-Änderungen – Änderungen, die nicht auf Link/Hardware-Fehler zurückzuführen sind, sollten einen misstrauisch machen.



Zwischenfazit: OSPF

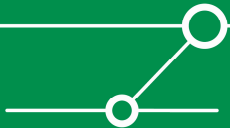
- **Bedrohungen & Schwachstellen existieren gegen OSPF.**
- **Angriffe sind auch nicht mehr rein theoretischer Natur.**
- **Geeignete “Mitigating Controls” ermöglichen den sicheren Betrieb – dazu zählen neben technischen auch organisatorische Massnahmen.**

- **Auditieren/Prüfen Sie ihre Infrastruktur.**



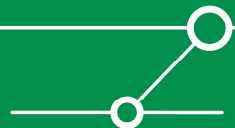
Exempli Gratia: HSRP

Hot Standby Router Protocol



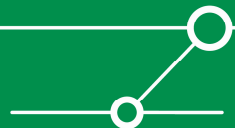
HSRP

- **Hot Standby Router Protocol**
 - Definiert in RFC 2281
- **Stellt Redundanz auf Router-Ebene zur Verfügung (“first hop redundancy”).**
- **UDP Port 1985**

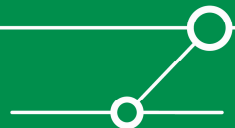
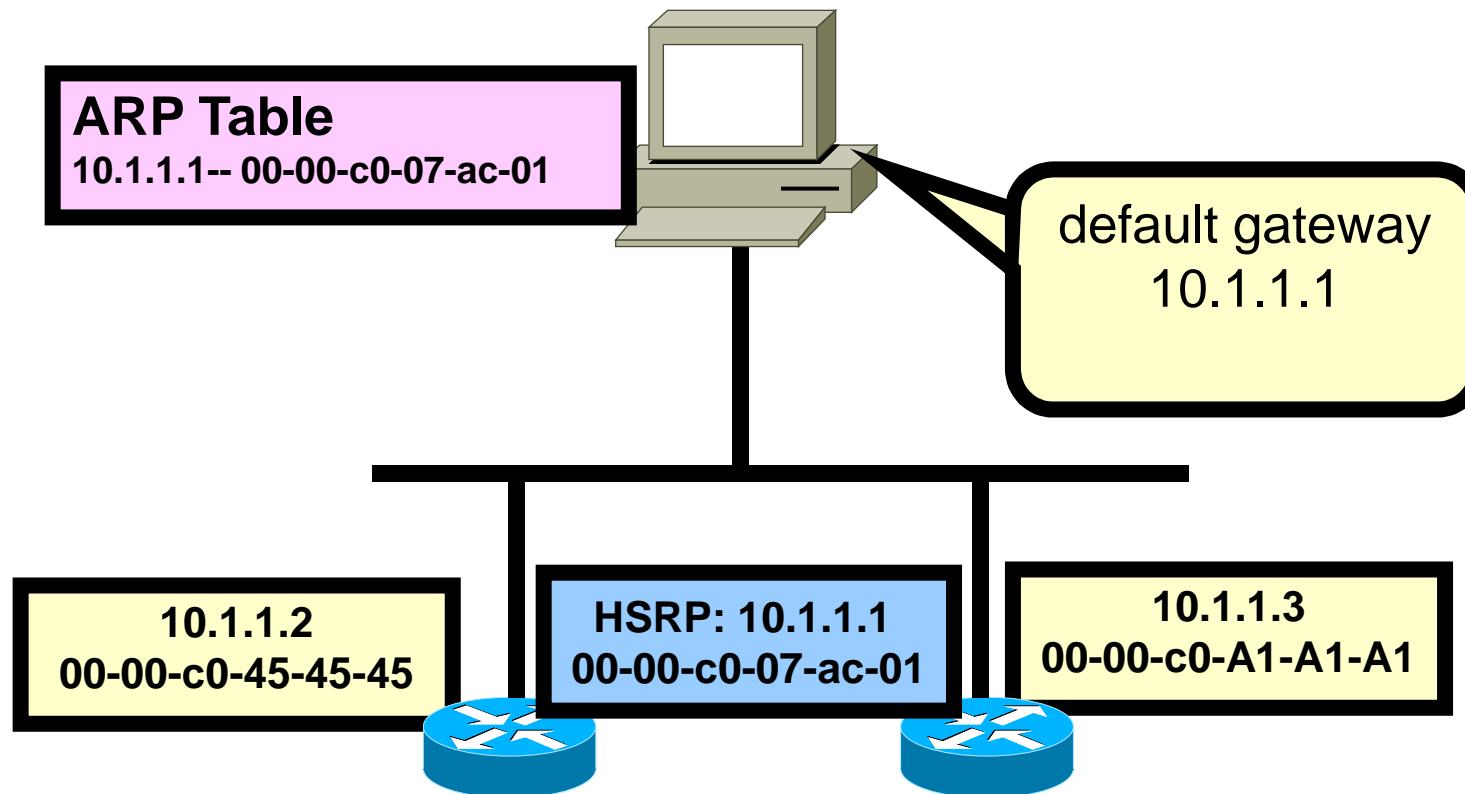


HSRP

- **Two or more routers can act as a single “virtual” router by sharing an IP and a MAC address.**
 - The members of the virtual-router group continually exchange status messages.
- **One router can assume the routing responsibility of another, if it goes out of service for either planned or unplanned reasons.**
 - Hosts continue to forward IP packets to a consistent IP and virtual MAC address, and the changeover between routes is transparent to the end workstation.

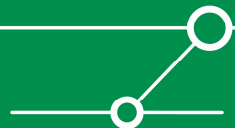


HSRP: virtuelle Router-IP



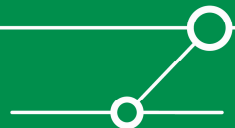
Active, Standby & Virtual

- Der **active router** leitet Datenpakete weiter und übermittelt “Hello”-Nachrichten an die anderen HSRP-Router.
- Der **standby router** monitort den Status des active router und übernimmt dessen Rolle, falls der active router nicht mehr verfügbar ist.
- Der **virtual router** ist wahrlich virtuell! Die virtuelle IP Adresse wird von allen HSRP- Routern geteilt, aber nur der active router reagiert darauf. Clients routen ihre Pakete zur virtual router Adresse

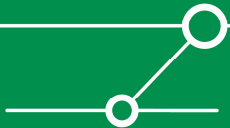


HSRP Nachrichten

- Werden zwischen den HSRP Routern ausgetauscht.
- **Sind per default nicht authentifiziert.**
- Dienen der Ermittlung des Active Routers.
- Werden als Multicast versendet: 224.0.0.2 (all routers).
- TTL der Pakete ist 1 – sie können also nicht geroutet werden.

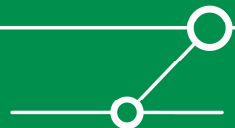


Threats & Vulnerabilites: HSRP



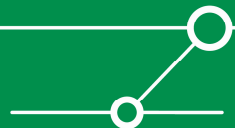
Threats HSRP

- **TH1: Angreifer wird Active Router und leitet Pakete nicht weiter – DoS**
- **TH2: Angreifer wird Active Router und leitet Pakete weiter – Sniffing/MitM – Verlust der Vertraulichkeit und Integrität**

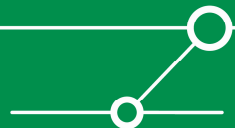


Vulnerabilities HSRP

- **VH1: Per default keine Authentifizierung**
- **VH2: Aufgrund des Protokolldesigns, werden HSRP-Nachrichten auf Access-Segmenten transportiert**
- **VH3: Klartext-Passwort-Authentifizierung transportiert Passwörter im Klartext auf Access-Segmenten**
- **VH4: MD5-Authentifizierung nur auf wenigen (sehr aktuellen) Endgeräten verfügbar**

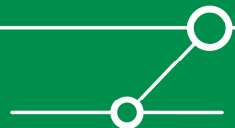


- Die Angriffe gegen HSRP sind denkbar einfach – und funktionieren zuverlässig mit Tools wie z.B. *yersinia* (<http://www.yersinia.net>)
- Ein Angreifer muss nur ein HSRP-Paket versenden, in welchem er eine höhere Priorität als alle anderen HSRP-Router der Gruppe reklamiert.

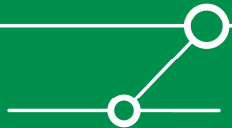


Mitigating Controls - HSRP

- **Wenn möglich, md5-Authentifizierung mit gutem Passwort verwenden.**
- **Per Design: “geschickte” Wahl der HSRP-Prioritäten _und_ Router-IP-Adressen kann die Angriffe massiv erschweren. (geschickt bedeutet: höchste Prio, Router haben die höchsten IP-Adressen im Segment)**

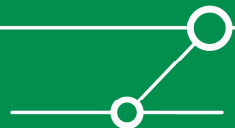


Zusammenfassung



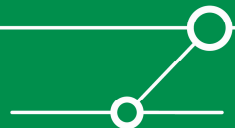
- **Vergessen Sie Ihre Infrastruktur-Security nicht – nur weil es gerade “out” ist ,-)**
- **Angriffe gegen Infrastruktur-Protokolle auf OSI-Layer2 und OSI-Layer3 sind Realität.**
- **Diese Angriffe kommen i.d.R. nicht übers Internet, sondern “von Innen” (was in der Natur der Angriffe liegt – sie funktionieren i.d.R. nicht über das Internet).**

- **Prüfen/Auditieren Sie auch die Infrastruktur.**



- <http://tools.ietf.org/html/draft-ietf-rpsec-ospf-vuln-02>
- RFC 4953: Generic Threats to Routing Protocols
- RFC 2328: OSPFv2
- CPAN: Net::Frame::Layer::OSPF (new)
- Yersinia (Angriffe gegen HSRP): www.yersinia.net

- Und für digitale Versionen des Vortrags und das Poc-Tool “OSPF-Attack-Shell”:
 - www.ernw.de



Vielen Dank...
Fragen? – Und Antworten

