Wirkungsanalyse von Routing-Angriffen im Internet

Master Seminar

Jan Henke

HAW Hamburg

14. November 2012

Outline

Outline

Outline

Outline

Erkentnisse aus AW1

- Für das Routing zwischen den Teilnetzten im Internet wird heute ausschließlich das Border Gateway Protocol(BGP)[1] genutzt
- Um den Routing-Graphen klein zu halten, verwendet BGP Autonome Systeme(AS) als Hierarchisierung
- BGP ist ein Pfadvektorprotokoll, transportiert daher neben dem next-Hop auch den kompletten bisherigen Pfad
- Jedes AS hat eine andere (lokale) Sicht auf den Rest des Internets
- Spezifiziert 1994 verfügt BGP über keine Mechanismen um dir Echtheit von Routen-Updates zu verifizieren

Erkentnisse aus AW1

- Für das Routing zwischen den Teilnetzten im Internet wird heute ausschließlich das Border Gateway Protocol(BGP)[1] genutzt
- Um den Routing-Graphen klein zu halten, verwendet BGP Autonome Systeme(AS) als Hierarchisierung
- BGP ist ein Pfadvektorprotokoll, transportiert daher neben dem next-Hop auch den kompletten bisherigen Pfad
- Jedes AS hat eine andere (lokale) Sicht auf den Rest des Internets
- Spezifiziert 1994 verfügt BGP über keine Mechanismen um dir Echtheit von Routen-Updates zu verifizieren

Erkentnisse aus AW1

- Für das Routing zwischen den Teilnetzten im Internet wird heute ausschließlich das Border Gateway Protocol(BGP)[1] genutzt
- Um den Routing-Graphen klein zu halten, verwendet BGP Autonome Systeme(AS) als Hierarchisierung
- BGP ist ein Pfadvektorprotokoll, transportiert daher neben dem next-Hop auch den kompletten bisherigen Pfad
- Jedes AS hat eine andere (lokale) Sicht auf den Rest des Internets
- Spezifiziert 1994 verfügt BGP über keine Mechanismen um dir Echtheit von Routen-Updates zu verifizieren

Erkentnisse aus AW1

- Für das Routing zwischen den Teilnetzten im Internet wird heute ausschließlich das Border Gateway Protocol(BGP)[1] genutzt
- Um den Routing-Graphen klein zu halten, verwendet BGP Autonome Systeme(AS) als Hierarchisierung
- BGP ist ein Pfadvektorprotokoll, transportiert daher neben dem next-Hop auch den kompletten bisherigen Pfad
- Jedes AS hat eine andere (lokale) Sicht auf den Rest des Internets
- Spezifiziert 1994 verfügt BGP über keine Mechanismen um dir Echtheit von Routen-Updates zu verifizieren

Erkentnisse aus AW1

- Für das Routing zwischen den Teilnetzten im Internet wird heute ausschließlich das Border Gateway Protocol(BGP)[1] genutzt
- Um den Routing-Graphen klein zu halten, verwendet BGP Autonome Systeme(AS) als Hierarchisierung
- BGP ist ein Pfadvektorprotokoll, transportiert daher neben dem next-Hop auch den kompletten bisherigen Pfad
- Jedes AS hat eine andere (lokale) Sicht auf den Rest des Internets
- Spezifiziert 1994 verfügt BGP über keine Mechanismen um dir Echtheit von Routen-Updates zu verifizieren

Angriffsmöglichkeiten auf BGP

- Zwei grundsätzliche Arten des Angriffs auf BGP:
  - Die Bindung von IP-Prefix und Origin-AS aufbrechen
    - Shortest Common Prefix Attack
    - Spoofed Origin Attack
  - Den AS-Pfad manipulieren
    - Shortest Valid Path, etc.

Angriffsmöglichkeiten auf BGP

- Zwei grundsätzliche Arten des Angriffs auf BGP:
  - Die Bindung von IP-Prefix und Origin-AS aufbrechen
    - Shortest Common Prefix Attack
    - Spoofed Origin Attack
  - Den AS-Pfad manipulieren
    - Shortest Valid Path, etc.

Angriffsmöglichkeiten auf BGP

- Zwei grundsätzliche Arten des Angriffs auf BGP:
  - Die Bindung von IP-Prefix und Origin-AS aufbrechen
    - ★ Shortest Common Prefix Attack
    - ★ Spoofed Origin Attack
  - Den AS-Pfad manipulieren
    - ★ Shortest Valid Path, etc.

Angriffsmöglichkeiten auf BGP

- Zwei grundsätzliche Arten des Angriffs auf BGP:
  - Die Bindung von IP-Prefix und Origin-AS aufbrechen
    - ★ Shortest Common Prefix Attack
    - ★ Spoofed Origin Attack
  - Den AS-Pfad manipulieren
    - ★ Shortest Valid Path, etc.

Angriffsmöglichkeiten auf BGP

- Zwei grundsätzliche Arten des Angriffs auf BGP:
  - Die Bindung von IP-Prefix und Origin-AS aufbrechen
    - Shortest Common Prefix Attack
    - Spoofed Origin Attack
  - Den AS-Pfad manipulieren
    - Shortest Valid Path, etc.

Angriffsmöglichkeiten auf BGP

- Zwei grundsätzliche Arten des Angriffs auf BGP:
  - Die Bindung von IP-Prefix und Origin-AS aufbrechen
    - ★ Shortest Common Prefix Attack
    - ★ Spoofed Origin Attack
  - Den AS-Pfad manipulieren
    - ★ Shortest Valid Path, etc.

Resource Public Key Infrastructre

- RPKI[2] 2012 standardisierte Infrastruktur zur Absicherung von BGP
- Sichert Bindung von IP-Prefix zu ASN kryptographisch ab
- Zertifikatshierachie entspricht Delegierung von Internet-Ressourcen (IANA -> RIR -> LIR)
- Deployment aktuell nicht sicher, da künstlicher Single-Point-of-Failure
- Kein Einfluss auf AS-Pfad basierende Angriffe

Resource Public Key Infrastructre

- RPKI[2] 2012 standardisierte Infrastruktur zur Absicherung von BGP
- Sichert Bindung von IP-Prefix zu ASN kryptographisch ab
- Zertifikatshierachie entspricht Delegierung von Internet-Ressourcen (IANA -> RIR -> LIR)
- Deployment aktuell nicht sicher, da künstlicher Single-Point-of-Failure
- Kein Einfluss auf AS-Pfad basierende Angriffe

Resource Public Key Infrastructre

- RPKI[2] 2012 standardisierte Infrastruktur zur Absicherung von BGP
- Sichert Bindung von IP-Prefix zu ASN kryptographisch ab
- Zertifikatshierachie entspricht Delegierung von Internet-Ressourcen (IANA -> RIR -> LIR)
- Deployment aktuell nicht sicher, da künstlicher Single-Point-of-Failure
- Kein Einfluss auf AS-Pfad basierende Angriffe

Resource Public Key Infrastructre

- RPKI[2] 2012 standardisierte Infrastruktur zur Absicherung von BGP
- Sichert Bindung von IP-Prefix zu ASN kryptographisch ab
- Zertifikatshierachie entspricht Delegierung von Internet-Ressourcen (IANA -> RIR -> LIR)
- Deployment aktuell nicht sicher, da künstlicher Single-Point-of-Failure
- Kein Einfluss auf AS-Pfad basierende Angriffe

Resource Public Key Infrastructre

- RPKI[2] 2012 standardisierte Infrastruktur zur Absicherung von BGP
- Sichert Bindung von IP-Prefix zu ASN kryptographisch ab
- Zertifikatshierachie entspricht Delegierung von Internet-Ressourcen (IANA -> RIR -> LIR)
- Deployment aktuell nicht sicher, da künstlicher Single-Point-of-Failure
- Kein Einfluss auf AS-Pfad basierende Angriffe

Erkenntnisse aus AW2

- Grundlage für derzeit verfügbaren Arbeiten ist das Topologiemodell von Lixin Gao[3] von 2001:
  - Hierarchische Strukturierung des Internets in Tier-1, Tier-2, usw.
  - Entwickelt auf Datenbasis von 2001 aus den USA
- Neuere Arbeiten[4] legen für das derzeitige Internet eine andere Struktur nahe
  - "Hyper-Giants" sehen ähnlich aus wie Tier-1-Provider, besitzen jedoch ein völlig unterschiedliches Peering-Verhalten
  - IXPs tragen dazu bei, dass sich das Internet immer stärker vermascht.

Erkenntnisse aus AW2

- Grundlage für derzeit verfügbaren Arbeiten ist das Topologiemodell von Lixin Gao[3] von 2001:
  - Hierarchische Strukturierung des Internets in Tier-1, Tier-2, usw.
  - Entwickelt auf Datenbasis von 2001 aus den USA
- Neuere Arbeiten[4] legen für das derzeitige Internet eine andere Struktur nahe
  - "Hyper-Giants" sehen ähnlich aus wie Tier-1-Provider, besitzen jedoch ein völlig unterschiedliches Peering-Verhalten
  - IXPs tragen dazu bei, dass sich das Internet immer stärker vermascht.

Erkenntnisse aus AW2

- Grundlage für derzeit verfügbaren Arbeiten ist das Topologiemodell von Lixin Gao[3] von 2001:
  - Hierarchische Strukturierung des Internets in Tier-1, Tier-2, usw.
  - Entwickelt auf Datenbasis von 2001 aus den USA
- Neuere Arbeiten[4] legen für das derzeitige Internet eine andere Struktur nahe
  - "Hyper-Giants" sehen ähnlich aus wie Tier-1-Provider, besitzen jedoch ein völlig unterschiedliches Peering-Verhalten
  - IXPs tragen dazu bei, dass sich das Internet immer stärker vermascht.

Erkenntnisse aus AW2

- Grundlage für derzeit verfügbaren Arbeiten ist das Topologiemodell von Lixin Gao[3] von 2001:
  - Hierarchische Strukturierung des Internets in Tier-1, Tier-2, usw.
  - Entwickelt auf Datenbasis von 2001 aus den USA
- Neuere Arbeiten[4] legen für das derzeitige Internet eine andere Struktur nahe
  - "Hyper-Giants" sehen ähnlich aus wie Tier-1-Provider, besitzen jedoch ein völlig unterschiedliches Peering-Verhalten
  - IXPs tragen dazu bei, dass sich das Internet immer stärker vermascht.

Erkenntnisse aus AW2

- Grundlage für derzeit verfügbaren Arbeiten ist das Topologiemodell von Lixin Gao[3] von 2001:
  - Hierarchische Strukturierung des Internets in Tier-1, Tier-2, usw.
  - Entwickelt auf Datenbasis von 2001 aus den USA
- Neuere Arbeiten[4] legen für das derzeitige Internet eine andere Struktur nahe
  - "Hyper-Giants" sehen ähnlich aus wie Tier-1-Provider, besitzen jedoch ein völlig unterschiedliches Peering-Verhalten
  - IXPs tragen dazu bei, dass sich das Internet immer stärker vermascht.

Erkenntnisse aus AW2

- Grundlage für derzeit verfügbaren Arbeiten ist das Topologiemodell von Lixin Gao[3] von 2001:
  - Hierarchische Strukturierung des Internets in Tier-1, Tier-2, usw.
  - Entwickelt auf Datenbasis von 2001 aus den USA
- Neuere Arbeiten[4] legen für das derzeitige Internet eine andere Struktur nahe
  - "Hyper-Giants" sehen ähnlich aus wie Tier-1-Provider, besitzen jedoch ein völlig unterschiedliches Peering-Verhalten
  - IXPs tragen dazu bei, dass sich das Internet immer stärker vermascht.

Traditionelle Sicht auf BGP-Angriffe

- Drei Akteure in jedem BGP-Angriff:
  - Ein Origin-AS für ein bestimmtes IP-Prefix
  - Eine Menge von "Client"-ASes, welche mit einer Adresse aus diesem IP-Prefix kommunizieren möchten
  - Ein Angreifer, welcher die Route von den "Client"-ASes zum Origin-AS manipulieren möchte
- Bisherige Sicht:
  - Angreifer versuchen einen möglichst großen Teil des gesamten Verkehrs von und zu einem IP-Prefix zu kontrollieren.

Traditionelle Sicht auf BGP-Angriffe

- Drei Akteure in jedem BGP-Angriff:
  - Ein Origin-AS für ein bestimmtes IP-Prefix
  - Eine Menge von "Client"-ASes, welche mit einer Adresse aus diesem IP-Prefix kommunizieren möchten
  - Ein Angreifer, welcher die Route von den "Client"-ASes zum Origin-AS manipulieren möchte
- Bisherige Sicht:
  - Angreifer versuchen einen möglichst großen Teil des gesamten Verkehrs von und zu einem IP-Prefix zu kontrollieren.

Traditionelle Sicht auf BGP-Angriffe

- Drei Akteure in jedem BGP-Angriff:
  - Ein Origin-AS für ein bestimmtes IP-Prefix
  - Eine Menge von "Client"-ASes, welche mit einer Adresse aus diesem IP-Prefix kommunizieren möchten
  - Ein Angreifer, welcher die Route von den "Client"-ASes zum Origin-AS manipulieren möchte
- Bisherige Sicht:
  - Angreifer versuchen einen möglichst großen Teil des gesamten Verkehrs von und zu einem IP-Prefix zu kontrollieren.

Traditionelle Sicht auf BGP-Angriffe

- Drei Akteure in jedem BGP-Angriff:
  - Ein Origin-AS für ein bestimmtes IP-Prefix
  - Eine Menge von "Client"-ASes, welche mit einer Adresse aus diesem IP-Prefix kommunizieren möchten
  - Ein Angreifer, welcher die Route von den "Client"-ASes zum Origin-AS manipulieren möchte
- Bisherige Sicht:
  - Angreifer versuchen einen möglichst großen Teil des gesamten Verkehrs von und zu einem IP-Prefix zu kontrollieren.

Traditionelle Sicht auf BGP-Angriffe

- Drei Akteure in jedem BGP-Angriff:
  - Ein Origin-AS für ein bestimmtes IP-Prefix
  - Eine Menge von "Client"-ASes, welche mit einer Adresse aus diesem IP-Prefix kommunizieren möchten
  - Ein Angreifer, welcher die Route von den "Client"-ASes zum Origin-AS manipulieren möchte
- Bisherige Sicht:
  - Angreifer versuchen einen möglichst großen Teil des gesamten Verkehrs von und zu einem IP-Prefix zu kontrollieren.

Traditionelle Sicht auf BGP-Angriffe

- Drei Akteure in jedem BGP-Angriff:
  - Ein Origin-AS für ein bestimmtes IP-Prefix
  - Eine Menge von "Client"-ASes, welche mit einer Adresse aus diesem IP-Prefix kommunizieren möchten
  - Ein Angreifer, welcher die Route von den "Client"-ASes zum Origin-AS manipulieren möchte
- Bisherige Sicht:
  - Angreifer versuchen einen möglichst großen Teil des gesamten Verkehrs von und zu einem IP-Prefix zu kontrollieren.

Idee für die Masterthesis

1. Untersuchung der Technologie- und Strukturänderungen auf Routing-Angriffe:
   - RPKI, was ist noch möglich, was nicht?
   - IXPs und Hyper-Giants, welche neuen Möglichkeiten bieten sich dort?
2. Untersuchung verschiedener Angriffsszenarien, die bis jetzt nicht beachtet wurden:
   - AS selektives Prefix-Hijacking

Idee für die Masterthesis

1. Untersuchung der Technologie- und Strukturänderungen auf Routing-Angriffe:
   - RPKI, was ist noch möglich, was nicht?
   - IXPs und Hyper-Giants, welche neuen Möglichkeiten bieten sich dort?
2. Untersuchung verschiedener Angriffsszenarien, die bis jetzt nicht beachtet wurden:
   - AS selektives Prefix-Hijacking

Idee für die Masterthesis

1. Untersuchung der Technologie- und Strukturänderungen auf Routing-Angriffe:
   - RPKI, was ist noch möglich, was nicht?
   - IXPs und Hyper-Giants, welche neuen Möglichkeiten bieten sich dort?
2. Untersuchung verschiedener Angriffsszenarien, die bis jetzt nicht beachtet wurden:
   - AS selektives Prefix-Hijacking

Idee für die Masterthesis

1. Untersuchung der Technologie- und Strukturänderungen auf Routing-Angriffe:
   - RPKI, was ist noch möglich, was nicht?
   - IXPs und Hyper-Giants, welche neuen Möglichkeiten bieten sich dort?
2. Untersuchung verschiedener Angriffsszenarien, die bis jetzt nicht beachtet wurden:
   - AS selektives Prefix-Hijacking

Idee für die Masterthesis

1. Untersuchung der Technologie- und Strukturänderungen auf Routing-Angriffe:
   - RPKI, was ist noch möglich, was nicht?
   - IXPs und Hyper-Giants, welche neuen Möglichkeiten bieten sich dort?
2. Untersuchung verschiedener Angriffsszenarien, die bis jetzt nicht beachtet wurden:
   - AS selektives Prefix-Hijacking

AS selektives Prefix-Hijacking

- Angriff auf ein bestimmtes “Client”-AS
- Angriffsziel primär “Eyeball”-Provider
- Ziel: Erschaffung einer Schatteninfrastruktur
- verborgen vor dem Rest des Internets

AS selektives Prefix-Hijacking

- Angriff auf ein bestimmtes “Client”-AS
- Angriffsziel primär “Eyeball”-Provider
- Ziel: Erschaffung einer Schatteninfrastruktur
- verborgen vor dem Rest des Internets

AS selektives Prefix-Hijacking

- Angriff auf ein bestimmtes “Client”-AS
- Angriffsziel primär “Eyeball”-Provider
- Ziel: Erschaffung einer Schatteninfrastruktur
- verborgen vor dem Rest des Internets

AS selektives Prefix-Hijacking

- Angriff auf ein bestimmtes “Client”-AS
- Angriffsziel primär “Eyeball”-Provider
- Ziel: Erschaffung einer Schatteninfrastruktur
- verborgen vor dem Rest des Internets

Das weitere Vorgehen

- Erstellung vollständiger Angriffsszenarios
- Vorhersage des zu erwartenden Ergebnisses
- Bestätigung durch das Sammeln von Daten:
  - Passiv: Auswertung der im Peeroskop gesammelten Daten
  - Aktiv: Durchführung eines Angriffes zur Datengewinnung
    - Testnetzwerk im Labor
    - Nutzung der für Testzwecke gedachten AS im Internet

Das weitere Vorgehen

- Erstellung vollständiger Angriffsszenarios
- Vorhersage des zu erwartenden Ergebnisses
- Bestätigung durch das Sammeln von Daten:
  - Passiv: Auswertung der im Peeroskop gesammelten Daten
  - Aktiv: Durchführung eines Angriffes zur Datengewinnung
    - Testnetzwerk im Labor
    - Nutzung der für Testzwecke gedachten AS im Internet

Das weitere Vorgehen

- Erstellung vollständiger Angriffsszenarios
- Vorhersage des zu erwartenden Ergebnisses
- Bestätigung durch das Sammeln von Daten:
  - Passiv: Auswertung der im Peeroskop gesammelten Daten
  - Aktiv: Durchführung eines Angriffes zur Datengewinnung
    - Testnetzwerk im Labor
    - Nutzung der für Testzwecke gedachten AS im Internet

Das weitere Vorgehen

- Erstellung vollständiger Angriffsszenarios
- Vorhersage des zu erwartenden Ergebnisses
- Bestätigung durch das Sammeln von Daten:
  - Passiv: Auswertung der im Peeroskop gesammelten Daten
  - Aktiv: Durchführung eines Angriffes zur Datengewinnung
    - Testnetzwerk im Labor
    - Nutzung der für Testzwecke gedachten AS im Internet

Das weitere Vorgehen

- Erstellung vollständiger Angriffsszenarios
- Vorhersage des zu erwartenden Ergebnisses
- Bestätigung durch das Sammeln von Daten:
  - Passiv: Auswertung der im Peeroskop gesammelten Daten
  - Aktiv: Durchführung eines Angriffes zur Datengewinnung
    - Testnetzwerk im Labor
    - Nutzung der für Testzwecke gedachten AS im Internet

Das weitere Vorgehen

- Erstellung vollständiger Angriffsszenarios
- Vorhersage des zu erwartenden Ergebnisses
- Bestätigung durch das Sammeln von Daten:
  - Passiv: Auswertung der im Peeroskop gesammelten Daten
  - Aktiv: Durchführung eines Angriffes zur Datengewinnung
    - Testnetzwerk im Labor
    - Nutzung der für Testzwecke gedachten AS im Internet

Das weitere Vorgehen

- Erstellung vollständiger Angriffsszenarios
- Vorhersage des zu erwartenden Ergebnisses
- Bestätigung durch das Sammeln von Daten:
  - Passiv: Auswertung der im Peeroskop gesammelten Daten
  - Aktiv: Durchführung eines Angriffes zur Datengewinnung
    - Testnetzwerk im Labor
    - Nutzung der für Testzwecke gedachten AS im Internet

Risiken

- Zeitbedarf
- Komplexität der Messungen
- Übertragung der Ergebnisse „in die freie Wildbahn“

Risiken

- Zeitbedarf
- Komplexität der Messungen
- Übertragung der Ergebnisse „in die freie Wildbahn“

Risiken

- Zeitbedarf
- Komplexität der Messungen
- Übertragung der Ergebnisse „in die freie Wildbahn“

Zusammenfassung

- Analyse von Bedrohungsszenarien auf BGP-Ebene
- Schaffung einer Wahrnehmung der Gefahr für AS-Betreiber
- Beschreibung neuer Angriffstechniken

Zusammenfassung

- Analyse von Bedrohungsszenarien auf BGP-Ebene
- Schaffung einer Wahrnehmung der Gefahr für AS-Betreiber
- Beschreibung neuer Angriffstechniken

Zusammenfassung

- Analyse von Bedrohungsszenarien auf BGP-Ebene
- Schaffung einer Wahrnehmung der Gefahr für AS-Betreiber
- Beschreibung neuer Angriffstechniken

Literatur


Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," IETF, RFC 4271, January 2006.


M. Lepinski and S. Kent, "An Infrastructure to Support Secure Internet Routing," IETF, RFC 6480, February 2012.


L. Gao, "On Inferring Autonomous System Relationships in the Internet," *IEEE/ACM Trans. Netw.*, vol. 9, no. 6, pp. 733–745, 2001.


C. Labovitz, S. Iekel-Johnson, D. McPherson, J. Oberheide, and F. Jahanian, "Internet Inter-domain Traffic," in *Proc. of the ACM SIGCOMM '10*. New York, NY, USA: ACM, 2010, pp. 75–86.

Literatur


Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," IETF, RFC 4271, January 2006.


M. Lepinski and S. Kent, "An Infrastructure to Support Secure Internet Routing," IETF, RFC 6480, February 2012.


L. Gao, "On Inferring Autonomous System Relationships in the Internet," *IEEE/ACM Trans. Netw.*, vol. 9, no. 6, pp. 733–745, 2001.


C. Labovitz, S. Iekel-Johnson, D. McPherson, J. Oberheide, and F. Jahanian, "Internet Inter-domain Traffic," in *Proc. of the ACM SIGCOMM '10*. New York, NY, USA: ACM, 2010, pp. 75–86.

Literatur


Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," IETF, RFC 4271, January 2006.


M. Lepinski and S. Kent, "An Infrastructure to Support Secure Internet Routing," IETF, RFC 6480, February 2012.


L. Gao, "On Inferring Autonomous System Relationships in the Internet," *IEEE/ACM Trans. Netw.*, vol. 9, no. 6, pp. 733–745, 2001.


C. Labovitz, S. Iekel-Johnson, D. McPherson, J. Oberheide, and F. Jahanian, "Internet Inter-domain Traffic," in *Proc. of the ACM SIGCOMM '10*. New York, NY, USA: ACM, 2010, pp. 75–86.

Literatur


Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," IETF, RFC 4271, January 2006.


M. Lepinski and S. Kent, "An Infrastructure to Support Secure Internet Routing," IETF, RFC 6480, February 2012.


L. Gao, "On Inferring Autonomous System Relationships in the Internet," *IEEE/ACM Trans. Netw.*, vol. 9, no. 6, pp. 733–745, 2001.


C. Labovitz, S. Iekel-Johnson, D. McPherson, J. Oberheide, and F. Jahanian, "Internet Inter-domain Traffic," in *Proc. of the ACM SIGCOMM '10*. New York, NY, USA: ACM, 2010, pp. 75–86.

Danke für die Aufmerksamkeit. Sind noch Fragen offen?