Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: INTERNET-DIENSTLEISTER

Sicherheit von Kabelnetzen und -routern

Über die bidirektionalen Kabelnetze stellen Internet-Service-Provider (ISP) nicht nur Fernsehen, sondern auch schnelle Internet-Zugänge sowie Telefonie zur Verfügung. Daher konnte in den vergangenen Jahren beobachtet werden, dass Internetanschlüsse zunehmend über diese Kabelnetze realisiert werden. Die Vielfalt an Diensten und die wachsende Anzahl der Kabelkunden sind somit Chance und Herausforderung zugleich.

Diese BSI-Veröffentlichung fasst wesentliche Aspekte zusammen, die zur Erhöhung der Sicherheit von Kabelnetzen und -routern beitragen. Hierbei sind die Schritte in prozess- und systemorientierte Maßnahmen untergliedert.

In dieser Cyber-Sicherheitsempfehlung werden die Verben „SOLLTE“ und „MUSS“ in ihren jeweiligen Formen sowie den zugehörigen Verneinungen genutzt, um deutlich zu machen, wie die jeweiligen Anforderungen zu interpretieren sind. Im Folgenden werden Sicherheitsmaßnahmen aufgeführt, die aus Sicht des BSI erfüllt werden MÜSSEN, um ein angemessenes Sicherheitsniveau nach dem Stand der Technik zu erreichen. Darüber hinaus werden Sicherheitsmaßnahmen dargestellt, die ebenfalls dem Stand der Technik entsprechen und aus Sicht des BSI grundsätzlich erfüllt werden SOLLTEN. Es kann aber Gründe geben, von einer gängigen Empfehlung abzuweichen, z. B. weil das Sicherheitsniveau durch andere Maßnahmen gewährleistet werden kann. Dies sollte jedoch sorgfältig abgewogen, stichhaltig begründet und dokumentiert werden.

1 Prozessorientierte Maßnahmen

Mithilfe von prozessorientierten Maßnahmen werden Aspekte der Informationssicherheit betrachtet, die den technischen Komponenten übergeordnet sind. Zu diesen Maßnahmen zählt u. a. die Einrichtung eines Sicherheitsmanagement, um wirksame Abläufe zur Herstellung von IT-Sicherheit bereitzustellen.[1] Des Weiteren greifen prozessorientierte Maßnahmen auch bei der Umsetzung von Sicherheitsanforderungen für organisatorische Prozesse. Diese Prozesse decken insbesondere auch personelle Aspekte wie das Identitäts- und Berechtigungsmanagement mit ab.[2] Sicherheitsaspekte, die sich mit dem Betrieb von IT-Komponenten befassen, sind ebenfalls von prozessorientierten Maßnahmen erfasst. Ein Teilbereich davon ist das Patch- und Änderungsmanagement.[3] Ein wichtiger Schritt zum sicheren und störungsfreien Betrieb stellt das Monitoring dar.[4] Diese Maßnahme ist um die zügige und effiziente Bearbeitung von Sicherheitsvorfällen zu ergänzen, um etwaige Schäden weitestgehend einzugrenzen. Für den Fall eines

1 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ISMS/ISMS_1_Sicherheitsmanagement.html
2 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_Uebersicht_node.html
3 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_Uebersicht_node.html
4 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/DER/DER_Uebersicht_node.html

Sicherheitsvorfalles SOLLTEN sowohl öffentliche als auch interne Kontaktdaten für Vorfallsmeldungen bereitgestellt werden. Schließlich MÜSSEN alle betroffenen internen und externen Stellen, wie beispielsweise die BNetzA oder das BSI, zeitnah informiert werden, sofern bei letzteren eine gesetzliche Meldepflicht gegenüber diesen Stellen besteht.[5]

2 Systemorientierte Maßnahmen

2.1 Kabelnetz

Das Kabelnetz ist in mehrere Segmente unterteilt. Dazu gehören auch das interne Provider-Netz sowie das Anschlussnetz, welches auch als Cable Television Netz (CATV-Netz) realisiert werden kann. Das CATV-Netz ist ein Shared-Medium, an dem auch die Kabelrouter und Cable Modem Termination Stations (CMTS) als entsprechende Gegenstelle angebunden sind.

Um die Anzahl der im Klartext übertragenen Informationen im CATV-Netz zu reduzieren, MUSS Early Authentication and Encryption (EAE) aktiviert werden. Dies hat zur Folge, dass die Kabelrouter umgehend nach der Aushandlung des Up- sowie Downstream-Kanals nur noch verschlüsselt mit der CMTS kommunizieren. Nachdem der Kabelrouter seine Konfigurationsdatei erhalten hat und eine Registrierung am CMTS erfolgt ist, MUSS Baseline Privacy Interface Plus (BPI+) als Verschlüsselung verwendet werden. Schließlich SOLLTE im CATV-Netz sowohl seitens des CMTS als auch des CM perfect forward secrecy (PFS) genutzt werden.

Kabelrouter sind als kompromittierbare Systeme zu behandeln. Folglich SOLLTE die CMTS als die erste tatsächliche Verteidigungslinie im Kabelnetz betrachtet werden. Daher MUSS auf jedem CMTS eine Access Control List (ACL) umgesetzt werden, um beispielsweise eine Separierung von Netzsegmenten zu realisieren und den Zugriff auf einzelne Dienste zu kontrollieren.

Die MAC-Adresse sowie das dazugehörige Zertifikat eines Kabelrouters können unter einem entsprechenden Aufwand geklont bzw. dupliziert werden. Dadurch ist eine nicht reguläre Identifikation sowie Authentifikation eines Gerätes am CMTS möglich. Ein Prozess zur Erkennung von Duplikaten MUSS mindestens täglich durchlaufen und die daraus resultierenden Ergebnisse ausgewertet werden. Sofern ein geklontes Gerät entdeckt wird, MÜSSEN Maßnahmen ergriffen werden, um dieses aus dem Kabelnetz auszuschließen. Dies kann beispielsweise dadurch erfolgen, indem das geklonte Gerät deprovisioniert und das entsprechende DOCSIS-Zertifikat widerrufen wird.

Sowohl im CATV-Netz als auch im internen Provider-Netz SOLLTE Dynamic ARP Inspection (DAI) verwendet werden, um Man-In-The-Middle Angriffe über ARP cache poisoning oder ARP spoofing Attacken zu verhindern. Darüber hinaus SOLLTE DHCP-Snooping eingesetzt werden, sodass die Wirkung von fremden oder bösartigen DHCP-Servern eingeschränkt wird. Zudem SOLLTEN in beiden Netzsegmenten geeignete Filterregeln aufgestellt werden, um MAC-Flooding Angriffe zu unterbinden.

Innerhalb des internen Provider-Netzes sind meist exponierte Systeme und Dienste vorzufinden, die sehr schützenswert sind. Der Zugriff auf diese Systeme und Dienste MUSS über eine sichere Identifikation sowie Authentifikation erfolgen. Sofern eine Authentisierung mithilfe eines Passwortes durchgeführt wird, MUSS ein individuelles Passwort mit einer hohen Passwortstärke (Länge und Komplexität) verwendet werden. Für die Passwortstärke SOLLTE eine Richtlinie erstellt werden. Alternativ MUSS eine Authentisierung mithilfe eines Zertifikats ermöglicht werden. Ferner SOLLTEN nur administrative Dienste verwendet werden, welche über eine verschlüsselte Verbindung kommunizieren. Beispielsweise SOLLTEN SSH, HTTPS oder SFTP anstelle von Telnet, HTTP oder FTP genutzt werden.

5 https://www.gesetze-im-internet.de/tkg_2004/__109.html

Die Administratoren MÜSSEN die verwendeten Systeme und Dienste angemessen härten, warten und dies dokumentieren. Hierzu MÜSSEN den Administratoren genügend Ressourcen bereitgestellt werden. Eine absolute Notwendigkeit für den sicheren Betrieb von IT-Komponenten ist beispielsweise das Einspielen von Sicherheitsupdates.

Um einen störungsfreien Betrieb auf Netzwerkebene zu gewährleisten, werden in internen Netzwerken Infrastrukturprotokolle, wie Spanning Tree Protocol (STP) und Hot Standby Router Protocol (HSRP), verwendet. Um Angriffe auf STP zu verhindern, SOLLTEN an allen Switches die Ports so konfiguriert werden, dass sie entweder überhaupt keine Bridge Protocol Data Units (BPDUs) entgegennehmen oder sich hinter dem jeweiligen Port keine STP-Root befindet. Alle verwendeten Infrastrukturprotokolle im internen Netzwerk SOLLTEN auf Anfälligkeiten für Angriffe überprüft werden.

2.2 Kabelrouter

Kabelrouter können gezielt angriffen werden, um einen Zugriff auf die Kommunikation im CATV-Netz zu erhalten. Es ist daher umso wichtiger, dass diese Geräte nach den Grundsätzen *security by design* und *security by default* entwickelt werden.

Die Installation einer manipulierten Firmware stellt eine potentielle Gefahr dar. Aus diesem Grund MUSS jedes Firmware-Update durch den Kabelrouter authentifiziert werden, bevor diese Datei hochgeladen und anschließend installiert wird. Ferner SOLLTEN Router-Hersteller ausreichend Ressourcen über einen Zeitraum von mindestens fünf Jahren einplanen, um diese Geräte zeitnah und in regelmäßigen Abständen mit Sicherheitsupdates zu versorgen.

Administrative Dienste wie Telnet DÜRFEN NICHT auf dem Kabelrouter zur Verfügung stehen. Falls dennoch administrative Zugänge erforderlich sind, MUSS eine sichere Alternative wie SSH verwenden werden, die eine Authentisierung und Verschlüsselung anbietet. Des Weiteren MUSS die Softwarearchitektur des Routers mehrere unabhängige Benutzer (multi-user) erlauben. Für die Nutzung einiger Kabelrouter-Funktionen ist kein voller Systemzugriff (root-Rechte) erforderlich. Um beispielsweise die Manipulation von Routen, Schnittstellen oder anderen System-Konfigurationen zu erschweren, SOLLTE eine rollenbasierten Zugriffskontrolle mit einem abgestuften Rechte-Konzept implementiert werden.

Um das Auslesen von Passwörtern im Klartext zu verhindern, MÜSSEN diese verschlüsselt gespeichert werden. Außerdem SOLLTE ein Trusted Platform Module (TPM) bereitgestellte werden. Sofern dieses Modul zur Verfügung steht, MÜSSEN sensible Daten, wie Passwörter oder auch Zertifikate, darin abgespeichert werden.

Allgemeine Empfehlungen zu Breitband-Routern, die beim Kauf bzw. bei der Miete beachtet werden sollten, sind in der BSI-Veröffentlichung „Sicherer Einsatz von Breitband-Routern“ aufgeführt.[6] Darin wird auch ein sicherer Betrieb von Routern beschrieben.

Dieses Dokument ist im Rahmen des Expertenkreises Internetbetreiber der Allianz für Cyber-Sicherheit entstanden. Mit den BSI-Veröffentlichungen informiert das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können an **info@cyber-allianz.de** gesendet werden.

6 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_131.html