Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.2.6 NTP-Zeitsynchronisation

1. Beschreibung

1.1. Einleitung

Vernetzte IT-Systeme erfordern oftmals synchrone Zustände. Meist dient die Uhrzeit als Referenz. Die interne Uhr von IT-Systemen kann jedoch von der tatsächlichen Zeit abweichen. Das Network Time Protocol (NTP) wird dazu verwendet, regelmäßig eine Referenzzeit zentraler Zeitgeber über Netzverbindungen zu ermitteln und die interne Uhr entsprechend anzupassen.

In Netzen erlaubt eine genaue Zeitsynchronisation Informationen mit einheitlichen Zeitstempeln zu versehen, z. B. um Daten chronologisch zu ordnen, Daten miteinander abzugleichen oder Zugriffsrechte zu befristen. Nur so lassen sich beispielsweise zeitliche Abläufe aus Protokolldaten verschiedener IT-Systeme miteinander in Beziehung bringen. Auch im Bereich der kryptographischen Protokolle sind genaue Zeitinformationen von Bedeutung. Darüber hinaus ist es in OT-Netzen essenziell, sämtliche Zeitgeber genau zu synchronisieren.

NTP-Clients beziehen Zeitinformationen von NTP-Servern. Die NTP-Server können wiederum als NTP-Clients Zeitinformationen von anderen NTP-Servern beziehen. So entsteht eine hierarchische Zeitverteilung (in sogenannte "Strata"). An der Spitze stehen NTP-Server, die ihre Zeit von genauen Quellen (z. B. einer Atomuhr, einem GPS- oder einem DCF77-Empfänger) beziehen. Diese NTP-Server werden als Stratum-1 bezeichnet.

Der NTP-Dienst nutzt Verfahren, um auch bei abweichenden Antworten verschiedener Zeitquellen die Abweichung der Systemuhr zu externen Zeitquellen zu bestimmen. Beispielsweise ignoriert er Zeitangaben einer Zeitquelle, die plötzlich gravierend von der eigenen Systemzeit abweicht.

Steuerungsnachrichten (Control Messages) erlauben es Clients, Statusinformationen abzufragen oder das Verhalten des NTP-Servers auch über das Netz hinweg zu ändern.

NTP-Nachrichten werden meistens ungesichert übertragen. NTP bietet jedoch die Möglichkeit, eine Nachricht mit kryptografischen Schlüsseln zu schützen, damit die Nachricht nicht unberechtigt verändert werden kann.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, NTP-Server und -Clients so abzusichern, dass die IT-Systeme im Informationsverbund verlässlich die Zeit ermitteln und ihre Uhren justieren können.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.2.6 *NTP-Zeitsynchronisation* ist auf jedes IT-System des Informationsverbundes anzuwenden, das NTP nutzt.

Um ein IT-Grundschutz-Modell für einen konkreten Informationsverbund zu erstellen, muss grundsätzlich die Gesamtheit aller Bausteine betrachtet werden. In der Regel sind mehrere Bausteine auf das Thema bzw. Zielobjekt anzuwenden.

Dieser Baustein behandelt

- die Planung zum Einsatz des NTP-Protokolls,
- den Betrieb von NTP-Servern sowie
- den Betrieb von NTP-Clients.

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- Allgemeine Anforderungen an den Betrieb von Servern (siehe SYS.1.1 *Allgemeiner Server*)
- Allgemeine Anforderungen an den Betrieb von Clients (siehe SYS.2.1 *Allgemeiner Client*)

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.2.6 *NTP-Zeitsynchronisation* von besonderer Bedeutung.

2.1. Unzureichende Planung des Einsatzes von NTP

Unzureichende Planung kann dazu führen, dass nicht alle IT-Systeme eine ausreichend genaue Systemzeit erhalten.

Wenn nicht richtig geplant wird, wie IT-Systeme ihre Systemzeit justieren können, dann können fehlerhafte Zeitinformationen in Anwendungen entstehen. Insbesondere zeitkritische Anwendungen können in der Folge fehlerhafte Zustände aufweisen oder ausfallen.

Beispielsweise kann ein Netz so segmentiert werden, dass NTP-Server und -Clients nicht mehr miteinander kommunizieren können. Zudem kann die unzureichende Planung der Zeitsynchronisation z. B. dazu führen, dass automatisierte Prozesse zu einem falschen Zeitpunkt ausgeführt werden.

2.2. Keine oder fehlerhafte Zeitinformationen

NTP-Server können ausfallen oder falsche Zeitinformationen übermitteln.

Wenn ein IT-System seine NTP-Server nicht mehr erreichen kann, weil diese ausgefallen oder nicht erreichbar sind, dann kann es seine Systemzeit nicht mehr justieren. Dadurch kann die Zeit der internen Uhr ungenau werden.

Falls ein NTP-Server fehlerhafte Zeitinformationen an NTP-Clients übermittelt, justieren diese möglicherweise ihre Systemuhr falsch. Dadurch können fehlerhafte Zeitinformationen in Anwendungen genutzt werden, beispielsweise in Protokolldaten.

Falsche Zeitinformationen können ebenfalls dazu führen, dass zertifikatsbasierte Dienste oder Dienste, die Einmalpasswörter verwenden, nicht mehr funktionieren. Infolgedessen können sich die Benutzenden nicht mehr auf IT-Systemen oder bei Netzdiensten anmelden.

2.3. Widersprüchliche Zeitinformationen

Zeitinformationen verschiedener Quellen können sich widersprechen.

Falls ein IT-System mehrere NTP-Server verwendet, um seine Systemuhr zu justieren, dann können die Zeitinformationen der verschiedenen NTP-Server unterschiedlich sein. Sobald die Zeitinformationen untolerierbar stark voneinander abweichen, kann das IT-System möglicherweise nicht mehr bestimmen, welche der Zeitinformationen die richtige ist. Dadurch kann die Systemzeit falsch justiert werden.

2.4. Manipulation der NTP-Kommunikation

Netzpakete mit Zeitinformationen können manipuliert werden.

Das NTP-Protokoll ist für verschiedene Angriffe anfällig. Bei einem Angriff können beispielsweise die Zeitinformationen manipuliert werden, während sie übertragen werden, oder NTP-Anfragen können zu einem anderen Server umgeleitet werden. So kann bei einem Angriff die Systemzeit der NTP-Clients manipuliert werden, um beispielsweise zeitlich beschränkte Zugriffsrechte zu nutzen, obwohl sie abgelaufen sind.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.2.6 *NTP-Zeitsynchronisation* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.2.6.A1 Planung des NTP- Einsatzes (B)

Der IT-Betrieb MUSS planen, wo und wie NTP eingesetzt wird. Dies SOLLTE vollständig dokumentiert werden. Dabei MUSS ermittelt werden, welche Anwendungen auf eine genaue Zeitinformation angewiesen sind. Die Anforderungen des Informationsverbunds hinsichtlich genauer Zeit der IT-Systeme MÜSSEN definiert und dokumentiert werden.

Der IT-Betrieb MUSS definieren, welche NTP-Server von welchen NTP-Clients genutzt werden sollen.

Es MUSS festgelegt werden, ob NTP-Server im Client-Server- oder im Broadcast-Modus arbeiten.

OPS.1.2.6.A2 Sichere Nutzung fremder Zeitquellen (B)

Falls Zeitinformationen von einem NTP-Server außerhalb des Netzes der Institution bezogen werden, dann MUSS der IT-Betrieb beurteilen, ob der NTP-Server hinreichend verlässlich ist. Der IT-Betrieb

MUSS sicherstellen, dass nur als verlässlich eingestufte NTP-Server verwendet werden. Der IT-Betrieb MUSS die Nutzungsregeln des NTP-Servers kennen und beachten.

OPS.1.2.6.A3 Sichere Konfiguration von NTP-Servern (B)

Der IT-Betrieb MUSS den NTP-Server so konfigurieren, dass Clients nur dann Einstellungen des NTP-Servers verändern können, wenn dies explizit vorgesehen ist. Darüber hinaus MUSS sichergestellt werden, dass nur vertrauenswürdige Clients Status-Informationen abfragen können.

Falls die internen NTP-Server der Institution nicht selbst hinreichend genaue Zeitquellen nutzen, dann MUSS der IT-Betrieb diese NTP-Server so konfigurieren, dass sie regelmäßig genaue Zeitinformationen von externen NTP-Servern abfragen.

OPS.1.2.6.A4 Nichtberücksichtigung unaufgeforderter Zeitinformationen (B)

Der IT-Betrieb MUSS alle NTP-Clients so konfigurieren, dass sie Zeitinformationen verwerfen, die sie unaufgefordert von anderen IT-Systemen erhalten.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

OPS.1.2.6.A5 Nutzung des Client-Server-Modus für NTP (S)

Der IT-Betrieb SOLLTE alle IT-Systeme so konfigurieren, dass sie den NTP-Dienst im Client-Server-Modus nutzen. NTP-Server SOLLTEN Zeitinformationen nur dann an Clients versenden, wenn diese aktiv anfragen.

OPS.1.2.6.A6 Überwachung von IT-Systemen mit NTP-Nutzung (S)

Der IT-Betrieb SOLLTE die Verfügbarkeit, die Kapazität und die Systemzeit der internen NTP-Server überwachen.

Der IT-Betrieb SOLLTE IT-Systeme, die ihre Zeit per NTP synchronisieren, so konfigurieren, dass sie folgende Ereignisse protokollieren:

- unerwartete Neustarts des IT-Systems,
- unerwartete Neustarts des NTP-Dienstes,
- Fehler im Zusammenhang mit dem NTP-Dienst sowie
- ungewöhnliche Zeitinformationen.

Falls der NTP-Server von sich aus regelmäßig Zeitinformationen versendet (Broadcast-Modus), dann SOLLTE der IT-Betrieb die NTP-Clients daraufhin überwachen, ob sie ungewöhnliche Zeitinformationen erhalten.

OPS.1.2.6.A7 Sichere Konfiguration von NTP-Clients (S)

Der IT-Betrieb SOLLTE festlegen, welche Zeitinformationen ein IT-System verwenden soll, wenn es neu gestartet wurde. Der IT-Betrieb SOLLTE festlegen, welche Zeitinformationen ein IT-System verwenden soll, wenn sein NTP-Dienst neu gestartet wurde.

Der IT-Betrieb SOLLTE festlegen, wie NTP-Clients auf stark abweichende Zeitinformationen reagieren. Insbesondere SOLLTE entschieden werden, ob stark abweichende Zeitinformationen von NTP-Servern nach einem Systemneustart akzeptiert werden. Der IT-Betrieb SOLLTE Grenzwerte für stark abweichende Zeitinformationen festlegen.

Der IT-Betrieb SOLLTE sicherstellen, dass NTP-Clients auch dann noch ausreichende Zeitinformationen erhalten, wenn sie von einem NTP-Server aufgefordert werden, weniger oder gar keine Anfragen zu senden.

OPS.1.2.6.A8 Einsatz sicherer Protokolle zur Zeitsynchronisation (S)

Der IT-Betrieb SOLLTE prüfen, ob sichere Protokolle zur Zeitsynchronisation eingesetzt werden können (z. B. Network Time Security (NTS)). Falls dies möglich ist, SOLLTEN sichere Protokolle eingesetzt werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.2.6.A9 Verfügbarkeit ausreichend vieler genauer Zeitquellen (H)

Falls korrekte Systemzeiten von erheblicher Bedeutung sind, dann SOLLTE eine Institution über mehrere Stratum-1-NTP-Server in ihrem Netz verfügen. Die IT-Systeme des Informationsverbunds mit NTP-Dienst SOLLTEN die Stratum-1-NTP-Server direkt oder indirekt als Zeitreferenz nutzen. Die Straum-1-Server SOLLTEN jeweils über verschiedene Zeitquellen verfügen.

OPS.1.2.6.A10 Ausschließlich interne NTP-Server (H)

Jedes IT-System des Informationsverbunds mit NTP-Dienst SOLLTE Zeitinformationen ausschließlich von NTP-Servern innerhalb des Netzes der Institution beziehen.

OPS.1.2.6.A11 Redundante NTP-Server (H)

IT-Systeme, bei denen die Genauigkeit der Systemzeit von erheblicher Bedeutung ist, SOLLTEN Zeitinformationen von mindestens vier unabhängigen NTP-Servern beziehen.

OPS.1.2.6.A12 NTP-Server mit authentifizierten Auskünften (H)

NTP-Server SOLLTEN sich bei der Kommunikation gegenüber Clients authentisieren. Dies SOLLTE auch für die Server gelten, von denen der NTP-Server seinerseits Zeitinformationen erhält. Die NTP-Clients SOLLTEN nur authentifizierte NTP-Daten akzeptieren.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein OPS.1.2.6 *NTP-Zeitsynchronisation* sind keine weiterführenden Informationen vorhanden.