Bild: Bürk Mobatime

Der Zeitserver DTS 4160 für Rechenzentren.

IT-Systeme in Kritischen Infrastrukturen

Sprünge in der Zeit verhindern

Stephan Herrmann

Das Thema IT-Sicherheit gewinnt im Bereich der Kritischen Infrastrukturen (Kritis) und der Öffentlichen Sicherheit zunehmend an Bedeutung. Gestohlene Nutzerdaten und Passwörter, weithin unbekannte Manipulationen im Darknet und vielfältige Hackerangriffe sind Schlagworte, die leider nur die Spitze des Eisbergs beschreiben.

Viele IT-Angriffe werden hingegen gar nicht öffentlich, künftige Bedrohungsszenarien sind nur sehr schwer abzuschätzen und stellen damit ein sehr komplexes, kaum noch greifbares Themengebiet dar.

In der Fülle all dieser Bedrohungen und Aufgaben wird oft übersehen, wie wichtig eine präzise Systemzeit für IT-Netzwerke und die Endgeräte ist. So weist das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem Maßnahmenkatalog „Hardware und Software“ darauf hin, dass „alle bei einem Vorgang betroffenen Rechner eine korrekte Zeitreferenz besitzen“ sollten. So sei dies „insbesondere bei der Auswertung von Protokollierungsinformationen […] von zentraler Bedeutung“, um zum Beispiel Fehlermeldungen, Synchronisierungsprobleme bei verteilten Systemen oder auch Dokumentationsaufgaben korrekt aufzulösen. Man spricht in der Praxis vom sogenannten Zeitstempel, der in der Regel mit der Verwendung des Network Time Protokolls einhergeht. Vielfach werden Kritis-Daten (zum Beispiel bei Energieversorgern, Wasserwerken, Krankenhäusern, Transport und Verkehr oder im Finanz- und Versicherungswesen) in Rechenzentren verarbeitet und gespeichert. Von Leitern derartiger Rechenzentren wird die Bedeutung einer präzisen und korrekten Systemzeit überwiegend bestätigt. Über die bereits genannten Gründe hinaus besitze die Zeit gar eine zentrale Bedeutung für die einwandfreie Funktion eines Rechenzentrums. Denn wenn die Zeitbasis nicht stimme, liefen die Softwareanwendungen tlw. nicht mehr zuverlässig und auch das Rebooten des IT-Systems sei dann sehr aufwändig. Und dies wiederum sei wichtig, da aufgrund der steigenden Anzahl von Cyberangriffen derartige Rebooting-Prozesse in der betrieblichen Praxis deutlich öfter durchgeführt werden müssen.

Sichere Zeitbasis im IT-Netzwerk

Das BSI bestätigt in seinen Schriften diese Auffassung und benennt drei mögliche Ausbaustufen, wie man eine zuverlässige Zeitbasis im IT-Netzwerk sicherstellen kann. In der niedrigsten Ausbaustufe würde zumindest eine Synchronisation des Computernetzwerkes durch NTP rmittels einer netzwerkbasierten Zeitquelle (zum Beispiel der Physikalisch Technischen Bundesanstalt) erfolgen. Hingegen stellt man in der mittleren Ausbaustufe bereits darauf ab, dass ein IT-Zeitserver, also ein entsprechend mit Quarzbasis und DCF-Funkantenne ausgestattetes Gerät, im Computernetzwerk als Zeitquelle integriert wird. Schließlich empfiehlt das Bundesamt als höchste Ausbaustufe, beim Empfangsgerät auf die Kombination von DCF- und GPS-Signalen zu gehen und auf einen hochpräzisen, internen Zeitgeber (Oszillator) zu achten. Man darf ergänzend festhalten, dass diese Empfehlungen bereits 2011 so formuliert wurden und sich die IT-Sicherheitslage seit dieser Zeit vermutlich weiter verschärft hat.

In der heutigen Praxis ist es daher so, dass man unter Umständen jedweden physikalischen Zugang zum Internet, etwa bei Nutzung eines Netzwerkdienstes, aus IT-Sicherheitsgründen kategorisch ausschließt. Auch würde man sich als IT-Verantwortlicher vermutlich die Frage stellen, ob denn diese „Zeit aus der Steckdose“ den hohen Ansprüchen im Rechenzentrum bezüglich System-/Geräteverfügbarkeit heute wirklich noch gerecht werden kann. Bei der mittleren Ausbaustufe wäre zu kritisieren, dass das DCF-Funksignal nicht unbedingt als manipulationssicher gilt, weshalb das BSI alternativ auch eine höhere Ausbaustufe mit entsprechender Differenzerkennung vorschlägt.

Unabhängig verbunden

Bei Kraftwerken hat sich mittlerweile eine hohe Ausbaustufe dergestalt als Standardlösung durchgesetzt, dass zwei lokale IT-Zeitserver mit präziser, interner Quarzbasis als NTP-/PTP- Zeitquellen im Computernetzwerk eingebunden sind. Beide Geräte sind unabhängig vom Netzwerk optisch miteinander verbunden und gleichen ihre Quarzbasis permanent zueinander ab. Dies ist notwendig, da jeder Oszillator eine noch so kleine Quarzdrift hat und sich daher beim Umschalten von einem Gerät auf das andere ein Zeitsprung ergeben könnte. Derartige Zeitsprünge sind in IT-Netzwerken technisch nicht verträglich. Diese hochwertigen Zeitserver sind darüber hinaus in der Lage, über eine einstellbare Plausibilitätsprüfung die jeweils eingehenden GPS-Zeitsignale zu verifizieren und im Falle von Störungen oder gar Angriffen diesbezügliche Fehlermeldungen abzusetzen.

Unter dem Strich deuten all diese technischen Argumente bei sachlicher Bewertung darauf hin, dass man derart präzise, sichere und hochverfügbare NTP-/PTP-Zeitdienstlösungen auch für IT-Systeme bei Kritis-Strukturen nutzen sollte.

Stephan Herrmann, geschäftsführender Gesellschafter der BÜRK MOBATIME GmbH, www.buerk-mobatime.de

Artikel als PDF für Abonnenten von Sicherheit.info Premium

www.sicherheit.info
Webcode: 2110043