Auch Energieversorger müssen sich jetzt auf Angriffe mit Hochleistungsrechnern vorbereiten.

geschrieben von Andreas Demmig | 30. Juli 2026

WuWT, Eddy Zervigon

Die US-Regierung ist zunehmend besorgt über das Potenzial von Angriffen mit Hochleistungsrechnern, die kommenden Quantencomputer. Im Juni unterzeichnete das Weiße Haus die Exekutivanordnung „ Sicherheit der Nation gegen fortgeschrittene kryptografische Angriffe “, um kritische Infrastrukturen, einschließlich der Energieversorgung, bei der Vorbereitung auf diese neue Bedrohungslage zu unterstützen.

Das Besorgniserregende an dieser Bedrohung ist, dass kryptografisch relevante Quantencomputer in der Lage sein werden, die Public-Key-Kryptografie zu knacken, die nahezu allem zugrunde liegt, was ein Kraftwerk oder eine Versorgungseinrichtung sichert, von verschlüsselten Daten über autorisierte Benutzer und Geräte bis hin zu Befehlen und Messwerten des Steuerungssystems.

Jüngsten Schätzungen zufolge könnten kryptografisch relevante Maschinen bereits im Jahr 2029 auf den Markt kommen, und dieser Zeitplan könnte sich noch weiter verkürzen, da Nationalstaaten Milliarden in den Wettlauf investieren .

Führungskräfte müssen diese Risiken jetzt priorisieren.

Jetzt ernten, später entschlüsseln

> Angreifer fangen heute verschlüsselte Versorgungsdaten ab und speichern sie, in der Hoffnung, sie mit Hilfe von Quantencomputern entschlüsseln zu können – eine Strategie, die als „Erfassen und späteres Entschlüsseln“ bekannt ist. Das Stromnetz ist ein ideales Ziel, da viele seiner Daten eine lange Lebensdauer haben: Einstellungen für den Relaisschutz, Konfigurationen der Anlagensteuerung, Steuerungsparameter von Generatoren und Turbinen, Netzwerktopologie und Verbindungsinformationen. Gestohlene Passwörter verfallen, aber die Informationen darüber, wie die Anlagensteuerung mit der Schaltanlage verbunden ist oder wie Umspannwerke mit der Leitwarte kommunizieren, bleiben erhalten.

Live-Überwachung

> Sobald Nationalstaaten Zugriff auf kryptografisch relevante Quantencomputer haben, könnte die grundlegende Sicherheit von Kommunikations-, Telemetrie- und Befehlsverbindungen – in manchen

Fällen nahezu in Echtzeit – gebrochen werden. Dies ermöglicht Angreifern einen permanenten Einblick in sensible Abläufe und erlaubt ihnen, genau zu sehen, wie diese Systeme funktionieren und wie sie diese sowie nachgelagerte Systeme am besten angreifen können.

Der Angriff auf die Datenintegrität

Wird eine Verschlüsselung geknackt, kann ein Angreifer physischen Schaden anrichten, ohne dass Insiderzugriff oder Software-Schwachstellen erforderlich sind. Er manipuliert einfach die Daten, die der Kontrollraum und seine Systeme erfassen. Dazu gehören SCADA-Telemetriedaten, Leistungsschalterstatus, Turbinendrehzahl, Spannung, Frequenz usw. Die Täuschung erfolgt auf zwei Arten: Entweder wird ein echtes Problem hinter scheinbar normalen Messwerten verborgen, während eine Maschine tatsächlich beschädigt wird, oder es wird ein Notfall vorgetäuscht, der Verwirrung stiftet und möglicherweise automatische Schutzmechanismen auslöst.

Sabotage und die ultimative Insiderbedrohung

Wenn die Public-Key-Verschlüsselung bricht, lässt sich nicht mehr zwischen einem externen Angreifer und einem vertrauenswürdigen Insider unterscheiden. Das bedeutet, dass bösartige Firmware, die mit einem gefälschten Zertifikat signiert ist, genauso aussieht wie ein legitimes Herstellerupdate. Ebenso erscheint ein gefälschter Befehl zum Auslösen eines Schutzschalters oder zum Deaktivieren des Generatorschutzes dem empfangenden Gerät als rechtmäßige Anweisung. In diesem Szenario übernimmt der Angreifer die Kontrolle über den Regelkreis. Die Folgen können gravierend sein, von Geräteschäden bis hin zu Stromausfällen.

Die Einsätze steigen dort, wo es kein Raster gibt.

Diese Risiken verstärken sich für eine schnell wachsende Kategorie von Einrichtungen: KI-Rechenzentren mit eigener, dedizierter Stromversorgung vor Ort. Diesen netzunabhängigen Systemen fehlt ein wichtiges Sicherheitsnetz. Fällt ein herkömmliches Kraftwerk aus, können benachbarte Kraftwerke und externe Versorgungsnetze die Auswirkungen abfedern, doch ein solches isoliertes Projekt verfügt über keine solche Absicherung. Ein Angreifer, der die Verschlüsselung der Telemetrie- und Steuerungsverbindungen dieses netzunabhängigen Systems knackt, kann sowohl die Stromversorgung vor Ort als auch das Rechenzentrum gleichzeitig lahmlegen.

Was die Energiewirtschaft jetzt tun muss

Hier sind einige Prioritäten für Führungskräfte:

Ergreifen Sie Maßnahmen für die offensichtlichen Probleme, noch bevor die Bestandsaufnahme abgeschlossen ist. Eine kryptografische

Bestandsaufnahme, die aufzeigt, wo sich Schlüssel und Zertifikate in OT- und IT-Umgebungen befinden, bildet die Grundlage jeder Migration zur Post-Quanten-Kryptografie (PQC), darf jedoch nicht zum Hindernis werden. Wenn bereits bekannt ist, dass ein Fernzugriffspfad oder eine Anbindung eines Anbieters quantenangreifbar ist, sollten parallel dazu Abhilfemaßnahmen eingeleitet werden. Sichern Sie jetzt die wichtigsten Verbindungen und identifizieren Sie gleichzeitig weitere Schwachstellen.

Priorisieren Sie nach Datenlebensdauer und -auswirkungen. Netztopologie, Schutzeinstellungen, technische Diagramme und andere wertvolle Informationen bleiben jahrzehntelang sensibel und werden bereits heute gesammelt. Daher sollten Daten zuerst geschützt werden, gefolgt von den Kanälen und Geräten, die physische Ausrüstung bewegen können.

Setzen Sie auf flexible Krypto-Architektur und nutzen Sie Overlays, wo ein vollständiger Austausch nicht möglich ist. Vermeiden Sie fest codierte Algorithmen und zentralisieren Sie stattdessen die kryptografische Verwaltung, sodass die Algorithmen bei der Weiterentwicklung von Standards ausgetauscht werden können. Hybride klassische und PQC-Kryptografie erleichtert den Übergang bei aufrüstbaren Geräten. Bei ressourcenbeschränkten Feldgeräten schützen Overlays wie die Schlüsselübermittlung außerhalb des regulären Datenverkehrs bestehende Verbindungen, ohne dass jeder Endpunkt neu konfiguriert werden muss. So bleibt der Systembetrieb ohne Ausfallzeiten gewährleistet.

Kompensieren Sie, was nicht aufgerüstet werden kann. Bei Geräten, die vor dem Austausch nicht quantensicher sind, stellen Sie sicher, dass eine strenge Segmentierung und ein Zugriffsprinzip mit minimalen Berechtigungen implementiert werden. Implementieren Sie quantensichere Gateways an den Schnittstellen und überwachen Sie die Systeme auf Anomalien, um den Aktionsradius eines Angreifers zu minimieren und die Dauer eines unbemerkten Eindringens zu verkürzen.

Die Post-Quanten-Bereitschaft sollte jetzt zur Beschaffungsvoraussetzung werden. Geräte, die in diesem Zyklus beschafft werden, werden auch nach dem Q-Day noch im Einsatz sein, daher wird ihre kryptografische Zukunft bereits mit der Bestellung festgelegt. Verträge sollten die finalisierten NIST-Standards , eine im Feld aktualisierbare Krypto-Agilität und eine kryptografische Stückliste vorschreiben.

Eddy Zervigon ist CEO von Quantum XChange.

Dieser Artikel wurde ursprünglich von RealClearEnergy veröffentlicht und über RealClearWire zur Verfügung gestellt.

https://wattsupwiththat.com/2026/07/23/power-operators-must-plan-now-for-four-quantum-attacks/

Persönliche Ergänzung

> Zu Zeiten als ich noch in der Industrie beschäftigt war, tauchte das Problem mit möglichen Hackerangriffen bereits auf. „In Mode“ kam damals Anfang der 90er Jahre, die Fernüberwachung und Wartung (Fehlerdiagnose und Up-date) von Rechner gesteuerten Anlagen, am liebsten Rund-um-die-Uhr und von der ganzen Welt aus, 24h Service eben.
>
> Meinen Kunden habe ich dann geraten, ihre Anlagen physisch vom Web abzuschalten – im einfachsten Fall mit einem Schalter, der nur vor Ort und manuell bedient werden kann. Ein stand-alone Rechnerklone, enthielt die identische notwendige SW und konnte vor Ort an die Anlage angeschaltet werden, und die aktuellen Anlagen Daten (ebenfalls) aufnehmen. Dieser Klone konnte dann ans Web geschaltet werden. Dieses hat oft bereits genügt, um mit diesem Klone eine Ferndiagnose zu ermöglichen. Nur die Servicetechniker vor Ort konnten die eigentliche Anlage bedienen, up-daten und reparieren.
>
> Das Ganze war natürlich umständlicher, aber der konventionelle Schalter konnte mit Sw nicht überwunden werden. Es war enorm, mit wie wenig „Fernabfragen“ die Anlagen dann eigentlich auskamen.

Sicherlich sind unter unseren Lesern Fachleute, die sich in diesem Thema besser auskennen als ich. Andreas Demmig