Sophos-Umfrage zu Cybersicherheit bei operativer Technologie

OT-Systeme waren bereits bei knapp der Hälfte der Betriebe Einfallstor für Cyberangriffe

Betriebe unternehmen viele Anstrengungen für die OT-Sicherheit, die meisten setzen zudem auf die Unterstützung externer Fachleute.
Die Mehrheit glaubt, dass OT-Systeme auch in Zukunft beliebte Ziele für Cyberangriffe sein werden, insbesondere im Bereich der Kritischen Infrastrukturen.

Maschinen, Anlagen und Systeme arbeiten zunehmend vernetzt, der Entwicklungsprozess ist dabei höchst dynamisch. Industry 4.0 und „Intelligente Fabriken" verändern die Produktionslandschaft in Höchstgeschwindigkeit. Gleichzeitig steigen hiermit die Risiken durch Cyberangriffe auf die Betriebstechnologien (Operational Technology, OT) und mit ihnen die komplexen Anforderungen an die OT-Security.

Sophos hat in einer DACH-weiten Umfrage bei 201 IT-Entscheidern, die mit den OT-Systemen in ihren Unternehmen vertraut sind, nachgefragt, inwieweit die Betriebe unter anderem abhängig sind von OT-Systemen und ob es bereits Angriffe darauf gegeben hat. Die befragten Unternehmen kamen zu über 80 Prozent aus dem Bereich der Industrie, die übrigen gehörten zum Versorgungssektor.

Hohe Abhängigkeit von OT-Systemen, knapp die Hälfte wurde bereits angegriffen
Die überwiegende Mehrheit der Betriebe bestätigte sehr stark (29,4 Prozent) oder stark (50,2 Prozent) von OT-Systemen abhängig zu sein. Teilweise auf Betriebstechnologien angewiesen sind 18,9 Prozent, kaum benötigt werden diese von 1,5 Prozent.

Dass diese Systeme bereits ein Ziel von Cyberkriminellen und angreifbar sind, beweist die folgende Zahl: 47,3 Prozent der befragten Unternehmen hatten bereits Cyberangriffe auf das Unternehmensnetzwerk zu verzeichnen, bei denen OT-Systeme von den Cyberkriminellen als Türöffner genutzt wurden. 44,3 Prozent der Betriebe hatten noch keinerlei Angriffsvarianten dieser Art zu bewältigen, 8,5 der Befragten konnten hierzu keine Angaben machen.

Viel (im) Einsatz für die OT-Sicherheit
Die beste Nachricht vorweg: Es sind nur 2,5 Prozent der Unternehmen, die angeben, überhaupt keine speziellen Maßnahmen für die Cybersicherheit ihrer OT-Systeme ergriffen zu haben. Die überwiegende Mehrheit hat bereits Maßnahmen und Lösungen im Einsatz – allen voran etwa Authentifizierungsmaßnehmen (58,7 Prozent) sowie Soft- und Firmware-Updates (57,7 Prozent). Firewalls und Intrusion Detection-Lösungen sind als Security-Maßnahmen zu 57,2 Prozent im Einsatz, gefolgt von VPN-Lösungen (51,7 Prozent), Sicherheitsschulungen für Mitarbeitende (49,3 Prozent) sowie das Blockieren unautorisierter Personen (48,3 Prozent). Weitere Maßnahmen, mit denen Unternehmen den Cyberschutz ihrer OT-Systeme stärken wollen, sind das Blockieren unautorisierter Anwendungen, Netzwerksegmentierungen sowie standardisierte Prozesse und Regeln. Schlusslichter der genannten Maßnahmen sind Schwachstellenanalysen und Penetrationstests, die lediglich von 31,8 Prozent der Unternehmen durchgeführt werden sowie physische Sicherheitsmaßnahmen, etwa Zugangskontrollen. Die Unternehmen konnten Mehrfachnennungen vornehmen.

„Für Unternehmen, deren OT-Systeme teilweise nicht mit einem klassischen Endpoint-Schutz ausgestattet werden können, ist es enorm wichtig, eventuelle offene Flanken schnell zu identifizieren, zu schließen und vor allem cyberkriminelle Aktivitäten im Netzwerk zu erkennen. Eine Schwachstellenanalyse und ein kontinuierliches Scannen des Netzwerks sind daher

unerlässlich. NDR-Lösungen identifizieren suspekte Verhaltensweisen im Netzwerk und tragen zudem mit der Erkennung unsicherer legitimer OT-Geräte zu einem erheblich höheren Schutzniveau bei“, sagt Michael Veit, Security-Experte bei Sophos.

Ein hohes Maß an externer Unterstützung
Die Mehrheit der Unternehmen setzt für die OT-Security auf externe Expertise. 18,4 Prozent haben ihre OT-Sicherheit komplett an Dienstleister ausgelagert und bei 46,3 Prozent der Unternehmen werden zumindest Teile der OT-Sicherheit von externen Spezialisten überwacht und betrieben. 12,9 Prozent der Betriebe planen innerhalb der nächsten 12 Monate eine Teil- oder Vollauslagerung ihrer OT-Sicherheit, während 22 Prozent angeben, sich um diesen wichtigen Punkt jetzt wie auch künftig inhouse zu kümmern.

Betriebe sehen in OT-Systemen künftige Ziele für Cyberkriminelle, allerdings eher bezogen auf Kritische Infrastrukturen
39,8 Prozent der Unternehmen sind überzeugt, dass OT-Systeme zunehmend lukrative Ziele für die Cyberkriminalität darstellen. 37,8 Prozent glauben allerdings, dass hierbei vor allem die Betriebstechnologien im Bereich der Kritischen Infrastrukturen im Fokus sein werden. Dass es einen Anstieg von Angriffen auf OT-Systeme zwar geben wird, hier aber im Vergleich zu klassischen IT-Systemen eine deutlich geringere Gefahr besteht, glauben 16,4 Prozent der Befragten. Lediglich eine Minderheit von 6 Prozent geht davon aus, dass OT-Systeme kein Cyber-Angriffsziel der Zukunft sind.

Über die Umfrage:
Techconsult hat im Auftrag von Sophos 201 IT-Entscheider und Entscheiderinnen zum Thema OT-Sicherheit in ihren Unternehmen befragt.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, Senior PR-Manager EMEA Central
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de