DCSO

THREAT DETECTION & HUNTING

Cyberangriffe auf Stadtwerke und lokale Versorger abwehren

Cyberangriffe auf Stadtwerke
und lokale Versorger abwehren

Aufgrund der wirtschaftlich herausfordernden Situation und des Fachkräftemangels sollten Stadtwerke und Versorger bemüht sein, die Effizienz ihrer Verteidigung gegen Cyberangriffe zu erhöhen. Dazu bietet es sich an, wiederkehrende Aufgaben auf externe Dienstleister zu verlagern. Diese Dienstleister sollten ein vollständiges Paket von Beratung über Detektion bis zur Hilfe im Notfall anbieten.

Stadtwerke und lokale Versorgungsunternehmen stehen in den letzten Jahren zunehmend im Fokus von Cyberangriffen. Zuletzt wurde Ende 2022 die Stadtverwaltung von Potsdam Opfer einer solchen Attacke und musste in diesem Zuge auch den Kundenservice der Stadtwerke temporär einstellen[1]. Die Wiederherstellung der Dienste dauert im Februar 2023 noch an.

> *Wir haben uns daher dazu entschlossen, die digitale Infrastruktur im Verbund temporär vom Netz zu nehmen und umfangreiche Untersuchungen zur Gewährleistung der Sicherheit eingeleitet. Während dieses Zeitraumes ist der Mailverkehr und auch die Aktualisierung der Webseite nicht möglich.*
>
> *Webseite der Stadt Potsdam*

Bereits 2020 war Potsdam Ziel eines Angriffs, der große Teile der Stadtverwaltung für eine Woche zurück in das analoge Zeitalter geschickt hatte.

Vermehrt im Fokus
von Angreifenden

Durch die Häufung der Angriffe in den letzten Jahren wird deutlich, dass auch kleinere und mittlere Versorger für Cyberkriminelle ein lohnendes Ziel darstellen. Es gibt aber auch Erfolge zu verzeichnen: Trotz zunehmender Schadensfälle ist das Kerngeschäft der Versorger, die Bereitstellung von Energie, Wasser und Mobilität selten betroffen. Dieser Trend ist auch auf verbesserte Abwehrsysteme zurückzuführen, die aus einer höheren Aufmerksamkeit für die Gefahren von Cyberangriffen resultieren.

Wie fragil dieser Erfolg ist, wird durch die Folgen des russischen Angriffskriegs auf die Ukraine deutlich: Der Krieg resultiert nicht nur in mehr und größeren Angriffen gegen kritische Infrastruktur in Deutschland[2], sondern setzt Versorgungsunternehmen auch einem Kostendruck in der Beschaffung von Gas und Öl aus. Allzu häufig steigen die Budgets für die Abwehr von Cyberangriffen in diesem kritischen Bereich nicht entsprechend der Gefahrenlage. Um weiterhin für die Sicherheit essenzieller Dienstleistungen zu garantieren, muss das Gebot der Stunde also sein, die Effizienz der Cyberabwehr zu erhöhen. Nur Effizienzgewinne erlauben es, trotz gleicher Ausgaben, das Schutzniveau weiter anzuheben.

Erfolgsfaktoren
für Cybersicherheit

Die Effizienz der Cyberabwehr hängt wesentlich von zwei Komponenten ab, die im Zusammenspiel funktionieren: den eingesetzten Tools und Produkten, sowie der Kompetenz derjenigen, die sie bedienen. Während sich die Produktlandschaft in den letzten Jahren stetig weiterentwickelt und Kunden davon automatisch profitieren, stellt gerade der Aspekt "Personal" für viele Versorger eine große Herausforderung dar. Dabei finden sich Versorger bei der Suche nach qualifizierten Fachkräften in Konkurrenz zu Unternehmen am freien Markt wieder, die anders wirtschaften und einstellen können.

Auch wenn es gelingt, Fachkräfte einzustellen, gibt es weitere Herausforderungen: Obwohl die Angriffe auf KRITIS-Unternehmen in den letzten Jahren stark zugenommen haben, sind sie auf ein einzelnes Unternehmen betrachtet immer noch recht selten. Dadurch bedingt ist es schwer, im seltenen Fall eines erkannten Angriffs Handlungssicherheit zu schaffen, für die ein konstantes Training notwendig ist.

Entlastung
durch externe Unterstützung

Eine Lösung für dieses Dilemma kann die Auslagerung von wiederkehrenden IT-Security-Aufgaben an externe Spezialist:innen sein. Dabei übernimmt der Dienstleister die personalaufwändige Bewertung von erkannten Angriffen und eliminiert "Falsch-Positive-Alarme".

Ist der Anbieter in der Lage weitere Systeme zur Angriffserkennung hinzuzufügen, um fortgeschrittene Angriffe zu erkennen, verbessert das die Qualität der Alarme, die an die Kunden gegeben werden. Liefern die Expert:innen direkt Handlungsempfehlungen mit, ermöglicht das einen effizienten Umgang.

Um beim eigenen Personal Kompetenzen aufzubauen, setzen viele Unternehmen auf Schulungen durch externe Anbieter. Diese bauen zumeist nicht auf reale Situationen im Unternehmen auf und ignorieren branchenbedingt Spezialfälle. Durch die Einbindung eines MSSP (Managed Security Service Provider)

Als 2015 gegründeter Managed Security Services Provider (MSSP) unterstützt die DCSO (Deutsche Cyber-Sicherheitsorganisation) Stadtwerke in Deutschland bei der Erkennung und Abwehr von fortgeschrittenen Cyberangriffen.
Dank der Nutzung komplementärer Systeme zur Angriffserkennung, die auf Basis von Netzwerkverkehr und Logdaten fortgeschrittene Angreifer erkennen, erhalten Kunden von der DCSO vorbereitete Alarme mit einer direkten Handlungsempfehlung. Dadurch steigt die Effizienz in der Abarbeitung und die Handlungssicherheit – ohne die Kontrolle über die eigene Umgebung abzugeben.

wie der DCSO lernen Mitarbeiter:innen dagegen am Beispiel realer Fälle. Die DCSO bietet dafür monatliche Fall-Gespräche mit SOC-Analyst:innen an, um an Alarmen aus den Kundensystemen die Einschätzung und Empfehlung des MSSP zu verstehen. Außerdem gibt es in allen Fallberichten die Möglichkeit für den Kunden, Kommentare zu hinterlassen und Fragen zu stellen, die durch das Team der DCSO beantwortet werden. Dadurch bauen die eigenen Mitarbeiter:innen Handlungssicherheit für unvorhergesehene Situationen auf.

Im Fall der Fälle
sicher aufgestellt

Sollte es zu einem Vorfall kommen, der mit eigenem Personal nicht zu bewältigen ist, bieten externe Incident Response (IR)-Anbieter Unterstützung bei der Organisation und technischen Wiederherstellung. Sinnvollerweise sollte diese Dienstleistung bei der Auswahl eines MSSP mit bedacht und gebucht werden, um im Notfall schnell kompetente Beratung zu erhalten. Anbieter wie die DCSO, die sowohl MSSP als auch IR-Leistungen (Incident Response) aus einer Hand anbieten, garantieren einen reibungslosen Übergang von der Detektion zur Wiederherstellung der Systeme. So sparen Sie im Notfall wertvolle Zeit.

Ein ganzheitlicher Ansatz
für mehr Sicherheit

Zum Leistungspaket der DCSO gehört auf Kundenwunsch auch die Beratung bei der Auswahl von Security-Produkten. In einem eigenen Testzentrum werden die Produkte auf Herz und Nieren geprüft. Zusätzlich zu diesen von Kunden gewählten Tooltests bietet die DCSO ergänzend eigene Sensorik an. Diese überwacht den Datenverkehr in den eingesetzten Kernnetzen auf der Suche nach unerkannten Angriffen und analysiert dazu Logdaten.

Gerade in heterogenen Umgebungen von Versorgern zahlt es sich aus, nicht nur auf eine einzelne Detektionskomponente zu setzen, sondern verschiedene Ansätze zu kombinieren. Die Komponenten der DCSO verursachen kaum zusätzliche Betriebsaufwände.

Mit einer Kombination aus eigener Kompetenz, sinnvoller Ergänzung durch Tools und Verlagerung arbeitsintensiver Aufgaben auf externe Dienstleister gelingt es lokalen Versorgern, trotz Kostendruck die IT-Sicherheit weiter zu steigern.

Lassen Sie sich gerne zum Angebot der DCSO beraten:
sales@dcso.de

Weitere Informationen zu Threat Detection & Hunting:
https://www.dcso.de/service/threat-detection-hunting/

Über die DCSO

Deutsche Cyber-Sicherheitsorganisation GmbH

Die DCSO Deutsche Cyber-Sicherheitsorganisation GmbH (DCSO) entwickelt moderne Cybersicherheits-Dienstleistungen für die deutsche Wirtschaft und bietet ihren Kunden darüber hinaus einen geschützten und herstellerneutralen Raum zum Austausch und der Zusammenarbeit in allen Fragen der Cybersicherheit.

Unter dem Dach der DCSO tauschen sich Unternehmen nicht nur untereinander, sondern auch mit Behörden und Forschungsinstituten über Cybersicherheitsgefahren aus. Die gewonnenen Erkenntnisse fließen in effektive Strategien und Lösungen für Prävention, Reaktion sowie Abwehr und sorgen so für mehr Sicherheit für Unternehmen, Wirtschaft und Gesellschaft.

Aus diesen Synergieeffekten der DCSO-Gemeinschaft und der eigenen Expertise entwickelt das Berliner Unternehmen moderne Managed Security Services in den Bereichen Bedrohungsidentifikation (Threat Intelligence), Monitoring und Detektion (Threat Detection & Hunting) sowie Hilfe zur Vorfallsbehandlung (Incident Response). Daneben unterstützt die DCSO Firmen mit Beratungsleistungen bei der Bewertung geeigneter Sicherheitstechnologien, der eigenen Cybersicherheit und der von Dienstleistern sowie beim Aufbau resilienter Business- und Informationssicherheitsprozesse.

Mit dem Ziel der Bedrohungen durch global organisierte Cyberkriminalität und staatlich gelenkte Wirtschaftsspionage entgegenzuwirken, wurde die DCSO 2015 von Allianz SE, BASF SE, Bayer AG und Volkswagen AG für die deutsche Wirtschaft gegründet.

Quellen:

[1] https://www.rbb24.de/politik/beitrag/2022/12/potsdam-cyber-angriff-verwaltung-stadtwerke-ermittlungen.html

[2] https://www.zdf.de/nachrichten/politik/cyber-angriffe-hacker-deutschland-ukraine-krieg-russland-102.html

DCSO Deutsche Cyber-Sicherheitsorganisation GmbH
EUREF-Campus 22
10829 Berlin, Germany

+49 30 - 72 62 19 - 0

www.dcso.de