GlitreNett

AUF CYBERANGRIFFE VORBEREITET

Wie Glitre Nett das richtige Angriffserkennungssystem für seine Netzwerke gefunden hat

Nach einer kürzlich durchgeführten Angriffssimulation hat sich Glitre Nett, der größte Verteilnetzbetreiber (VNB) in Südnorwegen, sehr lobend über die außergewöhnliche Performance unserer Lösung StationGuard geäußert. Unser Angriffserkennungssystem (Intrusion Detection System, IDS) war dank seiner robusten Fähigkeiten und effektiven Integration in kritische Infrastrukturumgebungen in der Lage, auch sehr komplexe Bedrohungen zu erkennen.

Der Teufel liegt immer im Detail

Umgeben vom rhythmischen Brummen der Computerlüfter und dem sanften Schein mehrerer Bildschirme saß Ozan zusammen mit seinem Team in seinem nur schwach beleuchteten Büro. Die Atmosphäre war angespannt – es hatte offenbar einen Cyberangriff gegeben und das Team war nun dabei, die Daten durchzugehen, um den Angriff zu verstehen.

Ozans Augen flogen über die Informationen auf seinem Bildschirm. Gleichzeitig dachte er an die jüngsten Angriffe auf kritische Infrastrukturen, wie etwa die Vorfälle im ukrainischen Stromnetz und die Angriffe auf Energieversorger in Dänemark. Diese Ereignisse erinnerten nur allzu deutlich an die ernüchternde Realität: Die Angriffe werden immer raffinierter, insbesondere was Steuerungssysteme betrifft. Er fragte sich, ob es sich bei den Angreifer:innen um unerfahrene Einzelpersonen handelte, die neue Angriffsvektoren ausprobierten, um Profis, denen es ums Geld ging, oder um die gefährlichsten aller Akteur:innen: staatlich gelenkt und mit den allerbesten Fähigkeiten und Ressourcen ausgestattet.

Plötzlich rief Christoph in die angespannte Stille: „Sieh dir das an!“ Ozan ging rüber zum Schreibtisch seines Kollegen. „Siehst du das? Dieses Gerät sendet nicht die erwarteten Daten.“ Wir haben Lücken“, stellte Christoph fest, während er sich durch die Bedienoberfläche des IDS StationGuard scrollte und den Steckbrief des betroffenen Geräts aufrief. „Hier! Und hier! Verdächtige Aktivitäten.“

Ozan vertiefte sich mit finsterer Miene in die Informationen vor ihm. „Was für verdächtige Aktivitäten?“ Christoph zeigte auf eine Reihe roter Alarmsymbole. „Nachdem die Verbindung wiederhergestellt wurde, hat das Gerät zur Validierung seiner IP-Adresse eine Gratuitous ARP ins Netzwerk rausgeschickt. Außerdem hat es versucht, eine Verbindung zum DHCP-Server herzustellen, und dabei eine automatisch generierte private IP-Adresse verwendet. Sieh dir die MAC-Adresse an.“

„Sieht so aus, als ob es versucht hat, die Verbindung nach dem Trennen wiederherzustellen.“

„Genau“, antwortete Christoph angesichts seiner Entdeckung ganz euphorisiert. „Das sieht für mich recht eindeutig nach einem Device-Replacement-Szenario aus. Das Gerät wurde geklont und manipuliert und das geklonte Gerät wurde anschließend wieder mit dem Netzwerk verbunden.“

„Sie wissen, dass das Auftauchen neuer IP-Adressen im Netzwerk einen Alarm auslöst, aber wenn sie ein Gerät einfach ersetzen und die IP- und MAC-Adresse spoofen, würden die meisten IDS das nicht erkennen.“ Ozan seufzte. „Das geht nur mit physischem Zugang zur Anlage. Das ist nicht einfach, aber auch nicht unmöglich. Besonders gefährlich ist das bei abgelegenen Schaltanlagen, zu denen nur alle paar Monate mal jemand hinfährt. Komm, wir sehen uns alle Geräte an, mit denen dieses geklonte Gerät in Kontakt war. Mal sehen, ob noch mehr Geräte kompromittiert wurden.“

Christoph fing an, die Liste vorzulesen: „Eine ausgenutzte Remote-Verbindung, ein tragbares Gerät, das von einem ahnungslosen Mitarbeitenden angeschlossen wurde, und jetzt ein physischer Angriff … Bist du die GOOSE-Meldungen durchgegangen?“

„Das ist einfach“, lächelte Ozan und ging an seinen Arbeitsplatz zurück. „Überprüfe du mal alle nicht autorisierten HTTP-Nachrichten, die an die Switches gesendet wurden.“

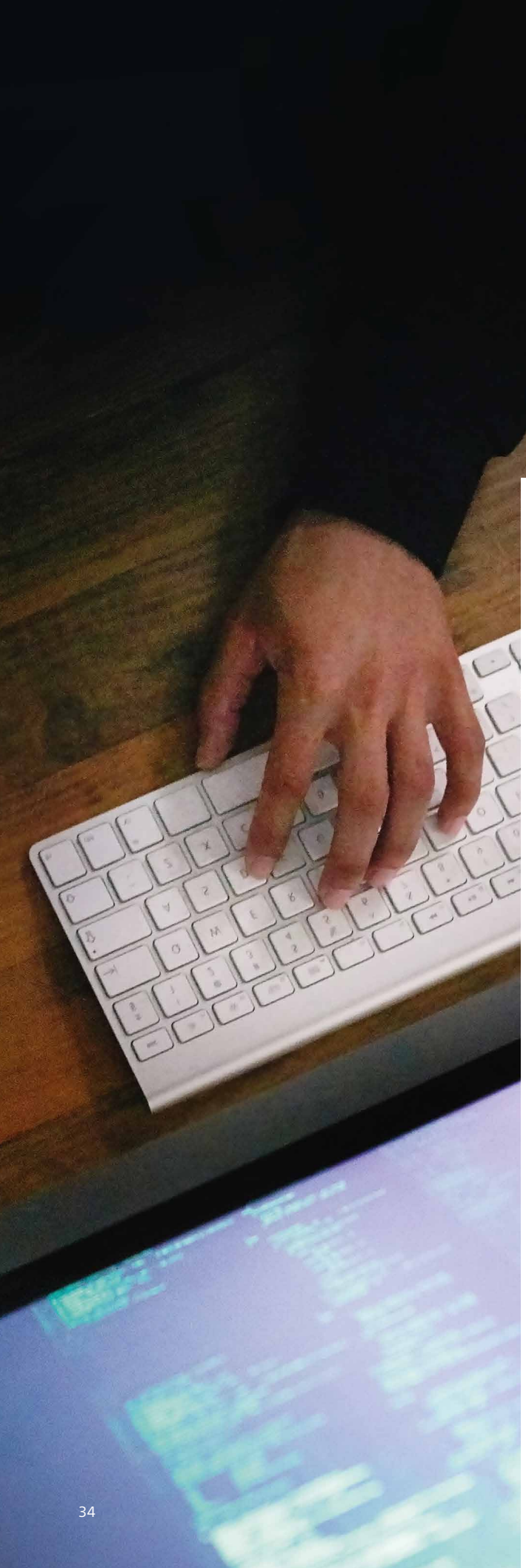
Christoph grinste: „Ich bin gespannt, was die Leute bei Glitre Nett bei dieser Angriffssimulation noch alles mit uns anstellen.“

Innovative Sicherheit

So oder so ähnlich könnte es sich bei der Analyse dieser Angriffssimulation abgespielt haben. Sehen wir uns diesen Test einmal genauer an. Wenn es um einen innovativen Ansatz für kritische Infrastrukturen geht, gilt Glitre Nett, der größte VNB in Südnorwegen, als Vorreiter. Atle Ripegutu, Leiter der Abteilung Process Control bei Glitre Nett, unterstreicht, wie wichtig diese proaktive Vorgehensweise ist: „Für Unternehmen im Bereich kritischer Infrastrukturen ist Innovation nicht einfach nur vorteilhaft, sondern unerlässlich. Es geht darum, proaktiv und vorbereitet zu sein. Die Aufräumarbeiten nach einem größeren Sicherheitsvorfall sind ein Albtraum. Vorab zu investieren ist zwar nicht billig, aber es verhindert spätere Ausgaben, die viel, viel höher sein können.“

***»Wenn das Stromnetz zehn Tage lang ausfällt, herrscht Anarchie.** Mit diesem Projekt wollten wir uns auf bedrohliche Szenarien wie dieses vorbereiten.«*

Vetle Norman,
System Engineer,
Glitre Nett



»Sie untersuchten Möglichkeiten, ***wie etwa das Eindringen in die Schaltanlage oder die Verwendung eines UDP-Traceroute, um die Netzwerktopologie zu ermitteln.«***

Aus diesem Grund beschloss Glitre Nett, Angriffserkennungssysteme zu testen und zu evaluieren. Dazu simulierte das Unternehmen reale Angriffe in seinen Schaltanlagen während des laufenden Betriebs. Die Lösungen, die evaluiert wurden, stammten von verschiedenen Anbietern. Das Unternehmen evaluierte für jedes System die Installations-, Konfigurations- und Erkennungsmöglichkeiten, die Skalierbarkeit und Flexibilität, die Bedienfreundlichkeit, die Genauigkeit der Alarme, das Reporting und die Effektivität des Supports.

Atle Ripegutu weist auf die besonderen Herausforderungen von Anlagennetzwerken im Vergleich zu Leitstellen hin: „Sobald man die Anlage verlässt und verschiedene Protokolle verwendet, gehen viele Informationen verloren, was das Monitoring und die Absicherung der Fernleitung erschwert." Angesichts veralteter Software, immer neuer IT-Anforderungen und der anstehenden Überführung der NIS 2-Richtlinie in das norwegische Recht ist die Nachfrage nach umfassenden IDS überwältigend.

Nach einer umfassenden Evaluierung wählte Glitre Nett die Lösungen von drei Kandidaten für die Teilnahme an der Angriffssimulation aus, darunter auch unsere.

Angriffssimulation bei laufendem Betrieb

Glitre Nett hatte zwar Bedenken, ein laufendes System zu testen, aber man kam zu dem Schluss, dass nur ein Real-World-Szenario wirklich akkurate Ergebnisse liefern kann. Vetle Norman, System Engineer bei Glitre Nett, kennt die Grenzen theoretischer Tests: „Forschungseinrichtungen, wie EFA in Norwegen, erstellen wertvolle theoretische Fallstudien, die jedoch oft nicht die Komplexität der tatsächlichen Vorfälle erfassen. Angriffe in der realen Welt laufen anders ab, und genau das wollten wir simulieren."

»Angesichts des kritischen Charakters der Infrastruktur war es nötig, ***selbst die unwahrscheinlichste Schwachstelle gründlich zu untersuchen.«***

VOM STATIONGUARD-SENSOR GEFUNDENE ANGRIFFSVEKTOREN

- Neue IP- und MAC-Adressen im Netzwerk
- Illegale MMS-Interaktionen
- Verschwundene GOOSE-Meldungen
- ARP-Spoofing
- NetBIOS-Reconnaissance-Aktivitäten einschließlich UDP-Traceroute, Ping-Sweeps und Port-Scans

Das Team um Vetle Norman konzentrierte sich auf die Nachstellung plausibler Einbruchsszenarien und Angriffsvektoren in ihren Schaltanlagen während des laufenden Betriebs. Sie untersuchten Möglichkeiten, wie etwa das Eindringen in die Schaltanlage, um dort eine manipulierte Komponente einzuschleusen, oder die Verwendung eines UDP-Traceroute, um die Netzwerktopologie zu ermitteln. Angesichts des kritischen Charakters der Infrastruktur war es nötig, selbst die unwahrscheinlichste Schwachstelle gründlich zu untersuchen.

Nachdem die Systeme aller Teilnehmer:innen installiert und eingerichtet waren, wurden alle Systemzugriffsverifizierungen implementiert und die Betriebsstabilität wurde bestätigt. Anschließend liefen die Systeme mehrere Monate lang autonom, sammelten dabei Daten und führten die ihnen zugewiesenen Aufgaben durch. Erst dann begann der Test.

Im Anschluss an die Angriffssimulation forderte Vetle Norman von jedem Anbieter eine detaillierte Analyse und entsprechende Empfehlungen auf der Grundlage der Ergebnisse an. „Wir mussten sehen, wie sich die einzelnen IDS unter realen Bedingungen geschlagen haben. Jedes Gewitter ist ein Test für die Belastbarkeit unserer Steuerungssysteme und Leistungsschalter. Dasselbe gilt für Angriffserkennungssysteme. Wenn nichts passiert, weiß man nicht, was die Systeme erkennen können“, so Vetle Norman. „Das war die Examensprüfung für OMICRON. Die Ergebnisse waren aufschlussreich und haben uns geholfen, Erkenntnisse über die Effektivität und die Lösungen unserer Hersteller zu gewinnen.“

Leistungsstarkes IDS für die detaillierte Analyse

Unser StationGuard-Sensor war von Ende 2022 bis Mitte 2023 in einer der Schaltanlagen von Glitre Nett installiert. Der Angriffssimulationstest fand an zwei aufeinanderfolgenden Tagen statt und keiner der teilnehmenden IDS-Anbieter kannte den Zeitpunkt des Tests und die Angriffsszenarien. Glitre Nett gab die gesammelten Daten erst nach Abschluss des Tests an die Anbieter heraus.

Unsere Herangehensweise an die Datenanalyse wird von einem multidisziplinären Team definiert, das sich aus OT-Ingenieur:innen und Protokollexpert:innen zusammensetzt, die sich mit IEC 61850 und IEC 104 auskennen. Ergänzt wird es durch Spezialist:innen aus dem Bereich IT-Cyber-Security. Die Bündelung des Wissens aus diesen verschiedenen Disziplinen ist unerlässlich, um ein möglichst breites Spektrum von Sicherheitsherausforderungen bewältigen zu können. „Dank unserer doppelten Expertise in den Bereichen Energiesysteme und Cyber Security können wir komplexe Probleme effektiv angehen“, so Ozan Dayanç, Cybersecurity Product Manager. „Die Zusammenarbeit zwischen IT und OT ist für eine robuste Reaktion auf Vorfälle unerlässlich, denn auf diese Weise können wir bei Alarmen und Vorfällen fundierte Entscheidungen treffen.“

Während des Tests sammelten StationGuard und dessen zentrales Managementsystem GridOps wichtige Daten aus dem Netzwerk von Glitre Nett. Glitre Nett hatte eine Remote-Verbindung zum StationGuard-Sensor eingerichtet, die es uns ermöglichte, auf die Konfigurationsdateien, Ereignisprotokolle und Packet Captures (pcaps) des Systems zuzugreifen. Anhand dieser Informationen analysierten wir die Systemkommunikation von Glitre Nett. Gleichzeitig half GridOps dabei, die Daten nach bestimmten Bereichen zu organisieren.

„Durch diese strukturierte Methodik konnten wir anhand der von uns beobachteten Muster und Anomalien verschiedene potenzielle Angriffe erkennen und kategorisieren“, erklärt Ozan.

„Eine erste Analyse ergab allgemeine Probleme wie nicht autorisierte Geräte, bekannte Angriffe wie TCP- und UDP-Port-Scans und ARP-Spoofing." Nachfolgende Analysen konzentrierten sich auf kompliziertere Vorfälle wie physische und Person-in-the-Middle-Angriffe. „Am Ende haben wir unsere Erkenntnisse in einem ausführlichen Bericht an Glitre Nett übergeben und waren dann gespannt, wie gut wir uns geschlagen haben", so Ozan.

Ergebnisse der Angriffssimulation

„Nach der Prüfung der Ergebnisse der Anbieteranalysen ist OMICRON aus dem Evaluierungstest als Sieger hervorgegangen. Ihre Lösung hat gewonnen – mit einem Erdrutschsieg", bestätigt Atle Ripegutu. StationGuard und das Team erkannten nicht nur 100 % der Angriffe und erstellten einen detaillierten Prüfbericht mit einer akkuraten Angriffszeitachse, sondern das OMICRON-Team war auch mit Abstand das schnellste.

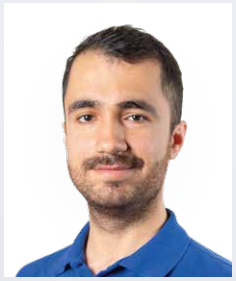
Auch Vetle Norman ist voll des Lobes, was den Erfolg unserer IDS-Lösung unterstreicht: „Ich möchte StationGuard in allen meinen Schaltanlagen", erklärte er. „Es war um Längen besser als alle anderen IDS. Zum einen geht das Konfigurieren überraschend mühelos. Einfach die Konfigurationsdatei hochladen und schon kann es losgehen. Zum anderen klappt das Zusammenführen von Geräten ganz reibungslos. Es ist möglich, eine Firewall, einen Netzwerk-Switch und ein Gateway in nur einem Gerät zu kombinieren, was perfekt ist." Auch die intuitive Bedienoberfläche hat es Atle Ripegutu angetan: „Ein System, das zwar Sicherheitsvorfälle erkennen kann, aber viel Training benötigt und schwer zu bedienen ist, ergibt betrieblich keinen Sinn für uns. Die Bedienung ist intuitiv, mit einfachen Befehlen zum Festlegen von Rollen und Kommunikationspfaden, was die Arbeit mit dem System zu einem Vergnügen macht."

Vetle Norman lobte auch die doppelte Ausrichtung von StationGuard auf Systemfunktionalität und Sicherheit: „StationGuard bietet eine Funktionsanalyse, die bei anderen Anbietern nicht zu haben ist. Es passt perfekt und der Einrichtungsaufwand ist minimal. Außerdem lässt es sich gut in SCADA-Systeme und RTUs integrieren. Soweit ich das einschätzen kann, bietet keine andere Lösung so ein Maß an Integration und die Leistungsfähigkeit."

Im Feedback von Glitre Nett fanden sich auch lobende Worte zu unserem Service und zur Einbindung der Kund:innen. „Sie haben in jeder Hinsicht eine vorbildliche Leistung erbracht – vom Umgang mit der Ausrüstung bis zur Unterstützung vor Ort. Alle Anfragen wurden sorgfältig bearbeitet, und jedes Problem wurde umgehend geklärt. Die Zusammenarbeit verlief außerordentlich reibungslos und kein einziges Problem blieb ungelöst", so Atle Ripegutu.

Eine vielversprechende Zukunft

Die Analyse des Angriffssimulationstests unterstreicht, wie wichtig ein IDS bei der Identifizierung von Cyberangriffen ist. „Erst durch das Testen außerhalb der Laborumgebung kann die tatsächliche Leistungsfähigkeit einer IDS-Lösung korrekt evaluiert werden", sagt Ozan. Die Evaluierung hat gezeigt, dass viele Bedrohungen von einem auf OT spezialisierten



»Es war eine tolle Erfahrung für uns. ***Der Test hat gezeigt, wozu unsere Lösung fähig ist, und er hat uns unsere Stärken und potenziellen Schwächen vor Augen geführt.«***

Ozan Dayanc,
Cybersecurity Product Manager,
OMICRON

GLITRE NETT

- Gründung: 2022 – Zusammenschluss von Agder Energi Nett (2000) und Glitre Energi Nett (1993)
- Hauptniederlassung: Drammen, Norwegen
- Beschäftigte: >350
- Elektrizitätskund:innen: >320 000

glitrenett.no

Angriffserkennungssystem wie StationGuard korrekt erkannt werden. Dabei kann schon ein einziger Alarm Hinweise auf einen ernsthaften Angriff geben.

Die Zusammenarbeit mit Glitre Nett war hervorragend. „Wir freuen uns auf die Fortsetzung unserer Partnerschaft und sind gespannt, wo sie uns hinführt", so Vetle Norman und er fügt hinzu: „Wir brauchen Ihren Support und Ihre Prüfausrüstung, um den derzeitigen Paradigmenwechsel zu bewältigen. Im Bereich der Cyber Security benötigen wir die einzigartigen Funktionen, die Ihre Systeme bieten. Wir möchten weiter eine enge Verbindung zu Ihnen pflegen und Sie einbeziehen. Wir möchten Ihre Ausrüstung auch in Zukunft einsetzen."

Unsere Lösung hat dem Team von Glitre Nett gezeigt, wie effizient sie ist. Und trotzdem gibt es, wie immer, Raum für Verbesserungen. „Wir haben ambitionierte Pläne für die Zukunft", sagt Ozan. „Wir arbeiten daran, unsere signaturbasierte Erkennung zu verfeinern, die Netzwerktransparenz zu verbessern und neue Sicherheitsfunktionen einzuführen. Auch Verbesserungen bei der Aufnahme des Anlageninventars stehen auf unserer Liste. Darüber hinaus werden wir weiterhin Innovationen voranbringen und uns an neue Bedrohungen anpassen."

Wenn Sie mehr über unser Angriffserkennungssystem StationGuard und das Schwachstellenmanagement erfahren möchten, besuchen Sie unsere Website unter

omicroncybersecurity.com/de/loesungen

PODCAST ZUM THEMA

Sie finden das Thema interessant?

In dieser Folge erfahren wir, wie ein OMICRON-Team von Cybersecurity-Experten eingehende Alarme analysiert und wie selbst die kleinsten Indikatoren versteckte Gefahren aufdecken, die die Sicherheit und den Betrieb eines ganzen Systems bedrohen. Scannen Sie den QR-Code oder besuchen Sie:

omicron.energy/episode79