Hinter dem Perimeter

Von Ripple20 bis Log4j – Netzwerke sind inhärent unsicher. Und jetzt?

narrowIN

Zurich University of Applied Sciences
zh aw School of Engineering

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Innosuisse – Swiss Innovation Agency

In den letzten Jahren haben Forscher eine erschreckende Anzahl von Schwachstellen gefunden, die weltweit hunderte Millionen Geräte betreffen – vom Internet-of-Things bis zu IT-Verwaltungsservern. Die Wahrscheinlichkeit, dass ein Unternehmensnetzwerk bereits unbemerkt kompromittiert wurde, ist hoch. Ein Umdenken von reaktiver zu proaktiver Netzwerksicherheit ist notwendig. In einem von der Innosuisse geförderten Projekt haben das Schweizer Netzwerk & Security Startup Narrowin und das Institut für Informatik (InIT) der ZHAW einen Exploration Node entwickelt, anhand dessen aufgezeigt werden kann, wie einfach und unbemerkt Angreifer agieren können, nachdem sie – beispielsweise durch Log4Shell – in ein Netzwerk eingedrungen sind.

Autoren

Dr. Tim Senn ist Mitgründer von Narrowin, einem universitären Spin-off im Bereich Netzwerk & Security.

tim.senn@narrowin.ch
https://narrowin.ch

Dr. Stephan Neuhaus ist Dozent für Informatik mit Schwerpunkt Sicherheit am Institut für angewandte Informationstechnologie der ZHAW.

stephan.neuhaus@zhaw.ch
https://zhaw.ch/de/engineering/institute-zentren/init/

Projektmitarbeitende

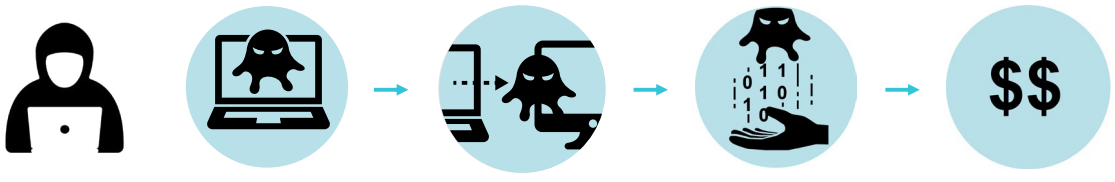
Mischa Diehm, Narrowin
Benjamin Gehring, ZHAW
Patrick Weber, Narrowin

Angreifer behalten den Zugriff auch nach der Schliessung einer Sicherheitslücke

Per Mitte Dezember 2021 wurden bereits mehr als 1.8 Millionen Attacken auf Basis von Log4JShell detektiert, von denen mehr als die Hälfte aller Unternehmensnetzwerke betroffen waren.[1] Gemäss dem Microsoft Threat Intelligence Center (MSTIC) hat ein breites Spektrum an Angreifern von hochprofessionellen staatlichen Akteuren bis hin zu einfachen Commodity Attackern die Schwachstelle ausgenutzt und weltweit Systeme kompromittiert. Dabei ist den meisten Organisationen nicht bekannt, ob bzw. dass sie selbst bereits betroffen sind.[2] Die Herausforderung ist, dass dies sehr schwierig festzustellen ist und zwischen initialer Kompromittierung und dem eigentlichen Angriff Monate vergehen können. Selbst wenn in dieser Zeit die Sicherheitslücke geschlossen wird, behält der Angreifer Zugriff auf das Netzwerk, denn Schwachstellen wie Log4Shell stellen nur das initiale Einfallstor dar: „Honestly, the biggest threat here is that people have already gotten access and are just sitting on it, and even if you remediate the problem somebody's already in the network … It's going to be around as long as the Internet.", so ein Senior Researcher des Cybersecurity-Unternehmens Sophos.[3]

Einmal im Netzwerk, sind die Angriffsvektoren vielzählig

Nachdem die Angreifer initialen Zugriff zum Netzwerk erhalten haben, haben sie Zeit. Über Monate wird langsam aufgebaut und aufgerüstet. Mittels Lateral Movement bewegen sie sich innerhalb des Netzwerksegments von Gerät zu Gerät und suchen nach Schwachstellen und geeigneten Angriffszielen. Viele Unternehmen detektieren dieses Verhalten nicht, da es in der normalen Kommunikation im Netzwerk untergeht. Wird am Ende dieser Zeit der eigentliche Angriff initiiert, geht es jedoch plötzlich nur noch um Minuten. Im Rahmen des Projekts wurden drei Angriffsmöglichkeiten näher beleuchtet.



Die zweite Verteidigungslinie in der modernen Angriffskette wird häufig unterschätzt.

Drei Angriffszenarien nach der initialen Kompromittierung

Option 1: Man-in-the-middle

Was ist es?
Ein Angreifer schafft es, sich zwischen Endpoint (vernetztes Gerät) und dessen Kommunikationsziele zu schalten und kann somit versuchen den Datenstrom mitzulesen oder diesen zu verändern.

Auswirkungen
Bei unverschlüsselter Kommunikation können z.B. Zugangsdaten mitgelesen werden. Diese können dann verwendet werden, um die Kontrolle über kritische Systeme zu übernehmen oder Schadcode zu hinterlegen.

Was braucht es?
Im Idealfall kann sich der Angreife so nahe am Endpoint wie möglich einklinken. Dazu hat er entweder direkten Zugriff auf z.B. das Netzwerkinterface des Endpoints oder ist im selben Netzwerk-Segment und schaltet sich dazwischen.

Learnings
- Es ist erstaunlich einfach, so einen Angriff unentdeckt zu durchzuführen, sobald man im Segment ist.
- Die Möglichkeiten zur Detektion sind sehr aufwendig und für Infrastruktur-Teams grosser Netzwerke nicht realistisch handhabbar. Zudem verhindern sie Attacken nicht und sind mit einer Reaktionszeit verbunden.

Was tun?
- Davon ausgehen, dass es passiert. Was mache ich dann?
- Risiko mitigieren. Wie kann ich den Impact minimieren? Beispielsweise durch Verschlüsselung, PVLAN sowie Segmentierung des Netzwerks.

Option 2: Denial-of-Service

Was ist es?
Ein Angreifer verhindert den Zugriff auf Ressourcen oder stört ganze Bereiche wie z.B. Netzsegmente. Dadurch wird der Geschäftsbetrieb gestört und es entsteht ein finanzieller Schaden.

Auswirkungen
Es kann zu langfristigen Ausfällen kommen, je nachdem wie gut versteckt diese DoS-Angriffe ausgeführt werden.

Was braucht es?
Diese Angriffe können insbesondere dann sehr einfach durchgeführt werden, wenn ein Angreifer einen Host im Netzsegment hat und auf diesem Administratorrechte hat.

Learnings
- Es ist sehr einfach, Basisservices wie z.B. DHCP, DNS und NTP oder Netzwerkinfrastruktur wie Switches zu kompromittieren.
- Sehr unauffällige, schlanke Attacke: Ein einzelnes Paket kann reichen, um ein System (z.B. einen Server) offline zu nehmen.

Was tun?
- First-Hop-Mechanismen aktivieren.
- Verschlüsselung ist eher unüblich in den gängigen Layer-2-Protokollen.
- Den Service an sich überwachen (z.B. DHCP-Monitoring). Hierfür bedarf es einer zentralen Logging-Infrastruktur (bspw. elastic).

Option 3: Exploit Vulnerability

Was ist es?
Ein Angreifer nutzt Schwachstellen in der Software, OS oder sogar der Hardware, um sich Zugriff zu verschaffen und mittels Lateral Movement auf mitunter kritische Infrastruktur zu gelangen.

Auswirkungen
Je nach Zugriffsrechten kann ein Angreifer unentdeckt persistenten Schadcode hinterlegen. Über diesen kann dann z.B. per Command and Control mit der Aussenwelt kommuniziert werden.

Was braucht es?
Der Angreifer den Zugriff auf das Zielsystem sowie eine passende Schwachstelle, um einen erfolgreichen Angriff durchzuführen.

Learnings
- Netzwerk-Segmente werden immer grösser und beinhalten eine Vielzahl unterschiedlicher Systeme. Dadurch wird es immer einfacher, in einem Segment Systeme zu finden, die direkt angreifbar sind.
- Ein gehacktes System kann lange unbemerkt schlummern, während der Angriff vorbereitet wird, um dann später z.B. für einen DoS-Angriff verwendet zu werden.

Was tun?
- Mikrosegmentierung verhindert Kommunikation von und zu kritischen Endpunkten.
- Aktives Schwachstellen-Scanning sowohl über das Netzwerk als auch direkt auf den Systemen (nessus, Rapid7, Microsoft Defender).
- Langfristig: Weiterführende Ansätze wie Zero Trust.

Ein Umdenken ist notwendig: Proaktive statt reaktive Netzwerksicherheit

Die Vielzahl an neuen Sicherheitslücken in grundlegenden Systemen macht es immer einfacher, Fernzugriff auf "interne" Netzwerke zu erlangen. Die vorliegende Analyse zeigt auf, wie einfach es ist, danach mittels unterschiedlicher Attacken erheblichen Schaden anzurichten.

Diese beiden Faktoren zusammengenommen demonstrieren, dass die reaktive Schliessung von bekannt gewordenen Sicherheitslücken keine nachhaltige Strategie zur Sicherung kritischer Netzwerke, Systeme und Daten ist. Die Lücken waren zum Zeitpunkt ihres Bekanntwerdens häufig schon seit Jahren ausnutzbar. Ein nachträgliches Patching ist zwar notwendig, hilft aber wenig, wenn die Angreifer bereits unentdeckt Systeme unter ihre Kontrolle gebracht haben. Stattdessen sind Netzwerksegmente und Systeme als inhärent unsicher zu betrachten und ihre Sicherheit durch proaktive Massnahmen wie eine Schutzbedarfsanalyse, eine Segmentierung des Netzwerks, die Mikrosegmentierung einzelner schützenswerten Geräte sowie die Erhöhung der Visibilität und gezieltem Monitoring und Alerting zu erhöhen.

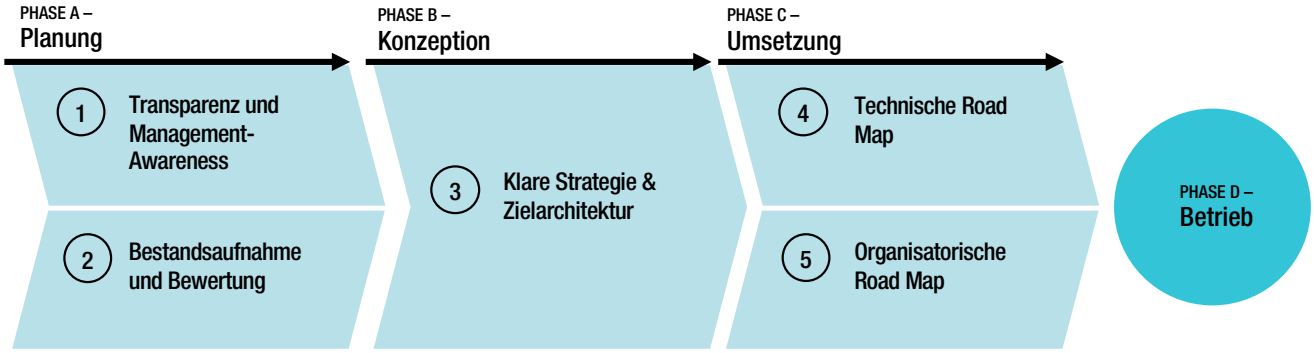
Durch eine strukturierte Bestandsaufnahme und Absicherung wird nicht nur die Sicherheit erhöht und die Möglichkeiten von Angreifern im Falle bereits kompromittierter Systeme eingegrenzt. Vielmehr wird auch im Betrieb die Transparenz und dadurch die Planbarkeit erhöht. Ohne diese proaktive Grundlagenarbeit werden sich die Notfalleinsätze bei jeder grösseren Sicherheitslücke wiederholen und Angreifer haben, wie im Projekt aufgezeigt, weitreichende Möglichkeiten auch nach der Schliessung der Lücken diverse Angriffe auszuführen.

Was hilft? Schritte zur Entwicklung einer sicheren Netzwerkarchitektur

Viele Netzwerke sind historisch gewachsen und ohne gesamtheitliche Sicherheitsbetrachtung konzipiert. Das Fehlen eines gesamtheitlichen Designs führt zu Silos, Effizienzverlusten und potenziellen Sicherheitslücken. Hinzu kommt ein unklares Zukunftsbild, das zunächst der Klärung der Anforderungen, der Evaluation bestehender Möglichkeiten sowie der Priorisierung von Handlungsfeldern bedarf. Auch das Zusammenspiel zwischen Cloud und eigener Infrastruktur ist zu klären.

Es gilt, diese Themen grundlegend anzugehen und eine durchdachte Zielarchitektur zu entwickeln. Statt auf einzelne Massnahmen zu fokussieren, erhöht eine solche Zielarchitektur nicht nur langfristig die Sicherheit, sondern

reduziert auch die Komplexität und erhöht die Kosteneffizienz für den Betrieb des Netzwerks und die Security.



Von der Planung bis zur Umsetzung ergeben sich dabei fünf Schritte:

1) Transparenz und Management-Awareness: Das eigentliche Problem ist häufig nicht technischer, sondern organisatorischer Natur. Fehlt das Bewusstsein und dadurch die Ressourcen, liegt der Fokus häufig auf technischen Einzelmassnahmen statt einer ganzheitlichen und langfristigen Verbesseung des Status Quo.

2) Bestandsaufnahme und Bewertung: Sind Bewusstsein und Ressourcen vorhanden, gilt es zunächst den Status Quo zu analysieren sowie die Handlungsfelder zu ermitteln und zu bewerten.

3) Klare Strategie & Zielarchitektur: Ausgehend von der Bestandsaufnahme kann ein technisches und organisatorisches Zielbild entwickelt werden. Dieses bietet die Grundlage, um einen IST-SOLL-Abgleich vorzunehmen und eine konkrete Road Map zu entwickeln.

4) Technische Road Map: Zur Umsetzung gilt es, die Abhängigkeiten zwischen verschiedenen Massnahmen und Technologien aufzuzeigen und konkrete Arbeitspakete abzuleiten. Diese werden in eine Zeitplanung überführt, die auch die Dringlichkeit und den Aufwand miteinbezieht. Konkrete Massnahmen zur Abwehr der beschriebenen Angriffsstrategien sind insbesondere Netzwerksegmentierung, der Aufbau von Sensorik / Visibilität sowie Mechanismen zur Authentisierung und Netzwerkzugangskontrolle.

5) Organisatorische Road Map: Neben dem Engagement und der Sensibilierung der Mitarbeitenden für die Thematik, kommt der Entwicklung klarer Rollen und Abläufe (Prozesse und Playbooks) eine zentrale Rolle zu. Technische Veränderungen sind nur mit entsprechenden organisatorischen Anpassungen wirksam.

Über das Projekt

Expedition Node: Für die Mini-Firewall von Narrowin wurde eine Software entwickelt, die es erlaubt, die Perspektive des Angreifers einzunehmen, der sich Zutritt zu einem Netzwerk verschafft hat.

Verweise

[1] https://blog.checkpoint.com/2021/12/11/protecting-against-cve-2021-44228-apache-log4j2-versions-2-14-1/

[2] https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/#attacks

[3] https://www.wired.com/story/log4j-log4shell-vulnerability-ransomware-second-wave/