Lateral Movement in Campusnetzwerken

Studie zu Herausforderungen und Lösungsansätzen

Im Dezember 2019 wird die IT-Infrastruktur der Universität Giessen und der Universität Maastricht weitgehend lahmgelegt und es dauert in beiden Fällen Monate, bis das IT-Netz wieder vollständig läuft. Die Universität Maastricht bezahlt dafür ein Lösegeld. Im Juni 2020 werden zahlreiche Forschungsarbeiten des Instituts für Medizin der University of California verschlüsselt und die Universität bezahlt auch hier nach intensiven Verhandlungen rund 1.14 Millionen US Dollar Lösegeld.

Lateral Movement in der modernen Angriffskette
Wesentlicher Bestandteil in der Angriffskette solcher Attacken ist „Lateral Movement". Dieses bezeichnet Techniken, mit denen sich Angreifer – von infizierten Geräten ausgehend – schrittweise durch ein Netzwerk bewegen und nach Schlüsseldaten und wichtigen Assets suchen. Dies können z.B. Forschungsdaten oder produktive Anlagen sein. Lateral Movement wird in heterogenen Netzwerklandschaften, wie die einer Universität oder eines Krankenhauses, durch den notwendigen Betrieb von legacy / locked Systems wesentlich begünstigt. Besonders in diesen Umgebungen ist das Verhindern von Lateral Movement eine sehr effektive und bisher wenig umgesetze Verteidigungsstrategie.

Ziel der Studie: Evaluation von Strategien zum Schutz kritischer Daten & Infrastruktur
Ziel ist es, die Treiber und Barrieren im Bereich Lateral Movement aus Organisationssicht besser zu verstehen. Zu diesem Zweck führen wir qualitative Interviews von ca. 45-60 Minuten mit Verantwortlichen der Universitäten durch. Im Zentrum stehen die folgenden Leitfragen:

- Ist Lateral Movement aktuell ein Thema? Wie wird das Gefahrenpotenzial eingeschätzt?
- Welche Ansätze sind bekannt bzw. werden umgesetzt?
- Was sind kritische Assets, die es zu schützen gilt?
- Was sind Anforderungen aus Organisationssicht an mögliche Lösungen?

narrowIN

Wir sind ein Startup mit universitärem Hintergrund. Uns begeistern komplexe Fragestellungen, für die wir nicht die umfassendste, sondern die sinnvollste Lösung suchen.

Kontakt: Tim Senn, tim.senn@narrowin.ch

Verteidungspunkte entlang der digitalen Angriffskette