Cybersecurity 2020: Prognosen und Tipps von Matthias Canisius, Regional Director CEE bei SentinelOne

Weitere Zunahme von Fileless-Malware

Die wirksame und zeitnahe Identifizierung von Schadsoftware ist heute eine der größten Herausforderungen der IT-Sicherheit in Unternehmen. Das liegt nicht zuletzt an der schieren Menge neuer Malware-Varianten – das BSI identifizierte im vergangenen Jahr 300.000 bis 400.000 neue Schadprogramme täglich – sondern auch an deren raffinierter Verschleierung, die herkömmliche Signatur-basierte Schutztechnologien überfordert. Ein zunehmend großes Problem ist dabei Fileless-Malware, die nicht an ausführbare Dateien gebunden ist und kaum bis keine Spuren auf der Festplatte hinterlässt. Vor allem Speicher-basierte Malware-Angriffe, sogenannte Memory-based Attacks, stehen bei Hackern hoch im Kurs. Dabei kommt Malware zum Einsatz, die im Hauptspeicher aktiv ist, dort Befehlskanäle einrichtet und dann selbständig Operationen ausführt, wie etwa das Herunterladen weiterer Trojaner. Prominente Vertreter von Fileless-Malware, die 2019 unter anderem mehrere deutsche Universitäten, Verwaltungen und Unternehmen infiziert haben, sind die Trojaner Emotet und Trickbot. Mit diesen werden wir auch im Jahr 2020 zu kämpfen haben, da wirksame Endpunktschutztechnologien noch immer nicht flächendeckend eingesetzt werden.

Steigendes Bedrohungspotenzial von MacOS

MacOS hat seit vielen Jahren den Ruf eines relativ angriffssicheren Betriebssystems. So gilt das OS von Apple als weit weniger anfällig für Malware und Cyberattacken als der Marktführer Windows. Obwohl der Großteil der Schadsoftware noch immer auf Windows und Linux abzielt, sollten auch Mac-User die Bedrohungslage nicht unterschätzen: Auch sie sind nicht immun gegen Kompromittierungen oder gefährliche Infektionen: Allein in den ersten sechs Monaten des Jahres 2019 identifizierten die Sicherheitsforscher von SentinelOne mindestens zehn verschiedene Arten von Malware, die speziell auf MacOS abzielen. Dabei zeigt sich die Tendenz, dass Cyberkriminelle die Mac-Plattform von Apple vermehrt fokussieren und auch immer häufiger Erfolg haben, weshalb im nächsten Jahr mit einem weiteren Anstieg mit MacOS-spezifischer Malware zu rechnen ist.

Ransomware wird personalisierter

Spätestens seit den groß angelegten, globalen WannaCry- und NotPetya-Kampagnen im Jahr 2017 wissen wir: Ransomware ist ein ernstzunehmendes Problem, das nur schwer unter Kontrolle zu bringen ist. Dies wird sich auch im Jahr 2020 nicht ändern, im Gegenteil: Wir sehen, dass Ransomware-Angriffe immer personalisierter und immer gezielter auf ihre Opfer ausgerichtet werden – sei es, dass Ransomware für spezielle Länder oder Branchen entwickelt wird oder die Angreifer gezielt besonders sensible, wertvolle oder brisante Daten verschlüsseln, anstatt unkontrolliert einfach alles zu codieren.

Automation wird in der Security unabdingbar

Security-Manager in Unternehmen stehen heute vor der großen Herausforderung, jeden Winkel ihres Netzwerks überwachen und schützen zu müssen – vom Endpunkt bis zur Cloud. Abteilungen, die dabei auf passive Bedrohungserkennung zurückgreifen, kommen schnell an ihre Grenzen, denn sie müssen eine schier

unendliche Zahl von Daten manuell in Zusammenhang bringen, analysieren und bewerten. In Zeiten von Fachkräftemangel, überarbeiteten IT-Teams und einer komplexen Bedrohungslandschaft ist dies eine Sisyphus-Arbeit. Deshalb sollten Schutzlösungen, die auf Automatisierung beruhen, auf der CI(S)O-Prioritätenliste für 2020 ganz oben stehen. Egal, ob es um Endpunktsicherheit, Passwort- und Identity-Management oder Datenanalyse geht, wenn Unternehmen ein Heer von Security-Experten für den Betrieb einer Lösung brauchen oder diese zeitaufwendig integrieren müssen, nützt die beste Lösung nichts.

Matthias Canisius, SentinelOne

Über SentinelOne
SentinelOne ist ein Pionier für autonomen Endpunktschutz und vereint die Prävention, Identifikation, Abwehr und Reaktion auf Angriffe jeglicher Art in einem einzigen Agenten. Dank dem Einsatz von künstlicher Intelligenz können Bedrohungen sowohl on-premises als auch in Cloud-Umgebungen automatisch und in Echtzeit eliminiert werden. Dabei ist die SentinelOne-Plattform ausgesprochen bedienerfreundlich und bietet eine herausragende Sichtbarkeit über alle kritischen Netzwerkvorgänge. Distributor in Deutschland, Österreich und der Schweiz ist Exclusive Networks.