heise Webcasts

Forcepoint

Inhalt des Live-Webcasts

Sicherer Umgang mit Dokumenten, ob E-Mail, Download oder Upload mit Zero Trust Content Disarm & Reconstruction

Datum und Uhrzeit: **22. November 2022, 11:00 Uhr**
Dauer: **ca. 60 Minuten**

Bei Cyber-Angriffen wird häufig Schadcode via Dokumente in Unternehmen geschleust. Content Disarm & Reconstruction von Forcepoint erkennt „guten" Inhalt aus einer eingehenden Datei, packt ihn in eine neue, saubere Datei und stellt diese dem User zu. Im Live-Webcast am 22. November um 11:00 Uhr erfahren Sie, wie Sie damit die Sicherheit Ihres Unternehmens verbessern können.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt Unternehmen auf seiner Webseite: „Für gezielte Angriffe werden häufig E-Mails mit Anhängen verwendet, die aufgrund des Themas, des Absenders und der Anrede die Wahrscheinlichkeit erhöhen, dass das potenzielle Opfer den Anhang öffnet. Typische Anhänge sind Dokumente, in denen ein Schadprogramm eingebettet ist." Dabei kann es sich um PDF-, Word-, Excel- oder PowerPoint-Dateien handeln. Die Frage, die Sie sich daher stellen sollten, lautet: **„Wie verhindere ich, dass schädliche Inhalte via E-Mail, über Downloads beim Surfen oder über den Upload im eigenen Karriereportal in mein Unternehmen gelangen?**

Die Antwort hierauf kann **Content Disarm & Reconstruction (CDR)** lauten. Dabei werden eingehende Inhalte/Dateien auf möglicherweise schädliche Bestandteile untersucht, diese im Verdachtsfall entfernt und der „saubere" Teil dann in eine neue Datei gepackt. Damit sollen sich eingehende Angriffe erkennen und verhindern lassen.

Einen Schritt weiter geht der Anbieter Forcepoint mit seinem Zero Trust CDR. Dabei gelten Dokumente per se als nicht vertrauenswürdig, es wird kein ausführbarer Code ausgeliefert. Die Lösung extrahiert aus sämtlichen Dateien in Sekundenbruchteilen die Nutzinformationen, wandelt sie in ein Zwischenformat um und verifiziert sie. Anschließend setzt sie daraus komplett neue Dateien im Ursprungsformat zusammen, die vollständig frei von ausführbarem Code sind und dadurch auch keine Schadsoftware mehr enthalten können. Dieses Verfahren kann die Technologie auf alle gängigen Dateiformate wie Office-Dokumente, Bilder oder PDFs anwenden.

So lassen sich nicht nur bekannte Angriffe und noch unbekannte eingehende Malware stoppen, auch das verdeckte Ausschleusen von Daten lässt sich unterbinden - selbst in Bilddateien via Steganografie eingebettete Inhalte werden erkannt.

Verschaffen Sie sich selbst einen Eindruck von der Wirksamkeit der Lösung! Matthias Senft, Senior Sales Engineer bei Forcepoint, erklärt Ihnen im Live-Webcast am 22.11. die Vorteile:

- maximaler Malware-Schutz im Umgang mit Dateien wie PDFs, Worddateien oder Bildern
- Schutz beim Upload, Download und E-Mail-Empfang
- höhere Sicherheit als Pattern-basierter Virenschutz dank Zero Trust

Er steht den Teilnehmern der Sendung zudem für Fragen zur Verfügung. Nutzen Sie diese Gelegenheit und informieren Sie sich! Moderator der Sendung ist Martin Seiler von Heise Business Services.

Sprecher:

Matthias Senft, Senior Sales Engineer, Forcepoint Deutschland GmbH

Matthias Senft is ein ehrfahrener technischer Presales Consultant und arbeitet seit vielen Jahren in der Cyber Security Branche. Er verfügt über eine große technische Expertise und fundiertes Wissen in den Bereichen Governance, Risk & Compliance, Information & Data Protection, Threat Protection und Defense.

Martin Seiler, Heise Business Services

Martin Seiler befasste sich als IT-Redakteur bei der Computerwoche viele Jahre lang mit Themen wie Netzwerke, Telekommunikation oder Security. 2006 wechselte er in den Eventbereich von IDG, für den er Fachveranstaltungen unterschiedlichster Art wie Seminare, Konferenzen, Roadshows und Webcasts entwickelte, organisierte und moderierte. Seit 2010 arbeitet Martin Seiler für Heise Business Services.