

Adaptive Redaction: Structural & Document Sanitization

Zwei Schlüsselkomponenten der Clearswift Adaptive Redaction-Technologie

Was ist Sanitization?

Unter Sanitization versteht man das Bereinigen oder Säubern von Dateien von gefährlichen versteckten Inhalten. Dies können aktive Inhalte (beispielsweise Malware) oder Informationen (wie versteckte Dokumenteigenschaften) sein. Schädlicher Code kann ein unsichtbares, bössartiges Skript auf einer ansonsten legitimen Webseite sein oder eingebettet in einem Dokument versteckt. Zur Beseitigung der Gefahr ist eine strukturelle Bereinigung (Sanitization) erforderlich. Versteckter sensibler Text kann beispielsweise in den Dokumenteigenschaften enthalten sein, die oft Benutzer- und Systemnamen sowie Revisionsinformationen enthalten. Ob versteckter Code oder sensible Informationen, beides muss entfernt werden, um Unternehmen vor möglichen Gefahren zu schützen. Sanitization ist eine der Optionen im Data Loss Prevention (DLP) Toolkit.

Die Funktionen für strukturelle Bereinigung und für Dokumentenbereinigung sind für die Clearswift Secure Gateways optional verfügbar und in ARgon enthalten.

Warum Sanitization?

Strukturelle Bereinigung (Structural Sanitization):

Aktive Inhalte gibt es überall. Sie ermöglichen Benutzern eine interaktive Erfahrung, entweder im Internet oder in einem Dokument. Hacker fügen jedoch ihre eigenen aktiven Inhalte in speziell dafür erstellte oder in kompromittierte Dokumente ein – beispielsweise in HTML-Dokumente zum Herunterladen oder in PDF-Dokumente, die als E-Mail-Anhänge verschickt werden. Diese Inhalte müssen erkannt werden. Da der aktive Code nur selten wichtig für die eigentlichen Informationen ist, sollte dieser möglichst immer entfernt werden.

Dokumentenbereinigung (Document Sanitization):

Viele Office-Dokumente enthalten versteckte Daten, die unter Umständen sensibel sind. Dies können die Dokumenteigenschaften sein, die sowohl den Autor als auch das tatsächliche Erstellungsdatum des Dokuments enthalten können, oder der Änderungsverlauf, der sensible Daten enthalten kann, von denen der Autor denkt, sie wurden entfernt – beispielsweise Projektdetails, neue Produktnamen oder Preise.

Die Bedeutung Automatischer Bereinigung

Die herkömmliche Methode für die Bereinigung von Dateien ist entweder eine manuelle Analyse oder das Löschen mit den Funktionen der Anwendung. Für beides können auch Lösungen von Drittanbietern eingesetzt werden. In allen Fällen ist der Erfolg jedoch abhängig vom Eingriff des Benutzers oder der IT-Abteilung - und das kann leicht übersehen werden.

Die Bereinigung ist eine Option, die in die Secure Gateways integriert und in ARgon enthalten ist. Da es sich hierbei um eine automatische serverseitige Option handelt, wird diese konsistent im gesamten Unternehmensnetzwerk angewendet und es ist weder eine Schulung noch ein Eingriff der Benutzer erforderlich.

Nur eine vollautomatische Bereinigung – wie sie mit den Clearswift-Lösungen möglich ist – bietet die Voraussetzungen für eine umfassende, konsistente, effiziente und vertrauenswürdige Bereinigung von Dokumenten.

Die Dokumentenbereinigung kann für das Erkennen und Entfernen sowohl der Dokumenteigenschaften als auch des Revisionsverlaufs für verschiedene Dokumentarten (inklusive PDF- und Office 2007+ Word-, Excel- und PowerPoint-Dateien) verwendet werden. Sie ist eine Schlüsselkomponente jeder Data Loss Prevention (DLP)-Lösung und verhindert, dass versteckte Daten das Unternehmen verlassen.

Strukturelle Bereinigung verwendet die Active-Content-Erkennungsregel und entfernt automatisch aktive Inhalte wie VBA-Makros aus Office-Dokumenten, JavaScript, VBScript und ActiveX aus HTML Nachrichtentext und HTML Anhängen, sowie JavaScript und ActiveX aus PDF-Dokumenten.

Adaptive Redaction

Adaptive Redaction ist DIE Technologie für einen proaktiven Ansatz, kritische Informationen zu schützen und damit zu verhindern, dass sensible Daten versehentlich nach außen oder innerhalb des Unternehmens in falsche Hände gelangen. Außerdem wird damit das Risiko durch Attacken von außen erheblich verringert. Als Eckpfeiler einer intelligenten DLP-Lösung bietet Adaptive Redaction eine Möglichkeit, die traditionelle Stop-und-Block-Methode zu umgehen und statt dessen nur die Inhalte automatisch zu entfernen, die gegen die Unternehmenspolicies verstoßen. Der Rest der Kommunikation und damit auch Ihr Tagesgeschäft kann ungehindert weiter gehen.

Adaptive Redaction entfernt auch potentiell gefährlichen, aktiven Content aus Dokumenten, bevor diese durch einen Mitarbeiter geöffnet werden. So umgehen Unternehmen das Risiko, das durch eingebettete APTs (Advanced Persistent Threats) entsteht. Die wichtigen Informationen erreichen ungehindert ihr Ziel, Malware wird entfernt.

Die Bereinigungsoption umfasst das Säubern von Dateien von gefährlichen Inhalten. Enthalten diese Inhalte versteckten oder verschleierte Code, kann dies zur Kompromittierung des Systems durch externe Personen führen. Neben des Verlusts geistigen Eigentums kann das auch eine Rufschädigung, mögliche regulatorische Maßnahmen sowie erhebliche Kosten für die Behebung der Systemverletzung nach sich ziehen. Die Bereinigungsoption von Clearswift vermeidet all dies automatisch, zentral, ohne Eingreifen durch Benutzer und ohne Auswirkungen auf die Unternehmensprozesse.



Fortra.com

Über Fortra

Fortra ist ein Cybersicherheits-Unternehmen wie kein zweites. Wir erschaffen eine einfachere und solidere Zukunft für unsere Kunden. Unsere bewährten Experten und unsere breite Palette integrierter und skalierbarer Lösungen bringen Ausgewogenheit und Kontrolle in Unternehmen auf der ganzen Welt. Bei Ihrer Reise zu mehr Cybersicherheit sind wir Ihr Wegbereiter und Ihr unermüdlicher Verbündeter auf jeder Etappe. Erfahren Sie mehr auf fortra.com/de.