RBI versus DNS Negativliste

Viele der sogenannten Next Generation Firewalls unterstützen DNS negative listing, das anhand von Webseitenkategorisierung und Sicherheitsinformationen den Zugriff auf Webseiten autorisiert während der Zugriff auf nicht vertrauenswürdige und unbekannte Seiten blockiert wird. Eine derartige digitale Entscheidung ist jedoch unzureichend.

Kompromittierung vertrauenswürdiger Webseiten

WebServer, Frames, aktive Komponenten, drive-by Downloads und Scripts vertrauenswürdiger WebSeiten können kompromittiert oder infiziert werden.

DNS Fakes

Der DNS Name einer vertrauenswürdigen Seite kann auf zwei Weisen kompromittiert werden:

- Der DNS Eintrag wird manipuliert und verweist auf einen Malware Server
- Ein Malware Server faked die IP eines vertrauenswürdigen Servers und missbraucht dabei den gültigen DNS Record

Zero Day Exploits

Neue Malware Server werden täglich tausendfach aktiv und gelten als so genannte Zero Day Exploits. Deshalb kann DNS negative listing den Zugriff auf solche Systeme nur generell zulassen oder blockieren - also keine wirklich qualifizierte Entscheidung treffen.

Unknown ist nicht zwangsläufig untrusted

Gleichfalls sind neue Webseiten häufig mit Zeitversatz oder überhaupt nicht in den Listen vorhanden, die für Kategorisierungen verwendet werden. Als „unknown“ eingestuft kann die Seite dann blockiert werden oder der Zugriff mit unbekanntem Risiko möglich sein.
Es läuft also bei solchen Zugriffen auf Einzelfallentscheidungen und manuelles Anlegen von individuellen Policies hinaus.

Administrativer Aufwand

Werden erforderliche Webseitenzugriffe blockiert löst dies einen administrativen Aufwand aus. Die Anwender öffnen ein Supportticket, die IT betrachtet und bewertet die Anforderung und erstellt gegebenenfalls Ausnahmeregeln. Neben dem damit verbundenen Aufwand mindert dies die Nutzungsqualität und Anwenderakzeptanz.

Datenexfiltration, Data Loss und Daten Up- und Download

DNS negative listing kann keine Datenexfiltration verhindern. Speziell weil DNS negative listing nur den Zugriff auf freigegebene Seiten erlaubt, jedoch keine funktionalen Regelwerke wie z. B. "Read-Only" Modus unterstützt.
Oftmals macht es Sinn als riskant kategorisierte Seiten zwar besuchen zu können, ohne jedoch Daten auf diesen zu hinterlassen (z. B. Formulare, Uploads) oder Daten von diesen zu beziehen (Downloads). Ein Datenabfluss über das Clipboard kann gleichfalls nicht unterbunden werden.

Übermittlung der Unternehmens IP

Web Zugriff über RBI übermittelt die IP Adresse der RBI Farm und NICHT die tatsächliche IP des Unternehmens. Diese Anonymisierung ist beim DNS negative listing Verfahren nicht gegeben.

Integritätscheck für Download Dateien

Hierzu sind in der Regel nachgeschaltete Instanzen erforderlich.

RBI hingegen ermöglicht die granulare Definition der auf eine Webseitenkategorie, einzelne Webseiten oder Multi-Domänen anzuwendenden Richtlinien.

Zugriff auf Webseite:	nein | ja
Nutzungsrestriktion:	Read-Only Modus | partieller Read-Only Modus
Datei upload:	nein | ja | ja unter Prüfbedingungen
Datei download:	nein | ja | ja unter Prüfbedingungen
Clipboard Unterstützung:	nein | ja | ja mit Einschränkungen
Zusatzfunktionen:	Umgang mit Cookies, Werbeblocker etc.
	Isolation virtueller Meetings

Fazit:

RBI bietet als skalierbare, granular abstimmbare Lösung einen hohen Schutzfaktor bei geringem technischen und administrativen Aufwand.
Die mehrschichtigen Einschränkungen und Schutzmassnahmen sind wirksam und erlauben dennoch eine hinreichend umfangreiche Internetnutzung.