

SECURE DNS

DNS-FILTERUNG, GEHOSTET IN DER
SCHWEIZ

**JEDE VERBINDUNG BEGINNT
MIT EINER DNS-ABFRAGE.**

An einem normalen Arbeitstag kontaktiert der Browser eines einzelnen Benutzers Hunderte von Domains, die niemand bewusst aufgerufen hat: Werbenetzwerke, Tracker, in andere Seiten eingebettete Inhalte. Einige davon verbreiten Phishing, Betrug oder Malware und wechseln ihren Namen so oft, dass die meisten Sperrlisten nicht nachkommen.

Viele Geräte im Netzwerk haben gar keinen Benutzer. Drucker, Kameras und OT-Steuerungen fragen rund um die Uhr Namen ab, und niemand prüft, welche.

Secure DNS beantwortet diese Abfragen über Resolver, die EXYS in der Schweiz betreibt. Jeder Name wird mit einer Datenbank schädlicher Domains abgeglichen, die EXYS täglich aus externen Feeds und eigenen Quellen neu aufbaut. Eine schädliche Domain erhält keine Antwort: Die Seite lädt nicht, und Malware erreicht ihren Server nicht.

Für die Umstellung ändern Sie nur die DNS-Einstellung in Ihrem Netzwerk. Installiert wird nichts, und jedes Gerät, das Namen abfragt, ist ab sofort geschützt.

**SCHÄDLICHE DOMAINS WECHSELN TÄGLICH DEN NAMEN.
UNSERE DATENBANK ZIEHT TÄGLICH NACH.**

BLOCKIERT, DGA

**Schädliche Anfrage an
q7vk2x0pzt4rl.top**

Von 10.20.40.17 im Servernetz,
08:14:03. Zwei weitere generierte
Namen folgten innert 50 ms.

NAMEN, DIE ES GESTERN NOCH NICHT GAB

Manche Malware hat keine feste Adresse für ihren Command-and-Control-Server. Sie erzeugt täglich viele zufällige Namen und probiert sie durch, bis einer antwortet; da kommt keine Liste mit. Secure DNS prüft deshalb auch den Namen selbst: Mit Sprachverarbeitung (NLP) erkennt es generierte Namen, auch solche, die noch nie aufgetaucht sind.

WAS SIE SEHEN

Sie erhalten täglich einen Bericht per E-Mail, der auch im Portal abrufbar ist. Er zeigt, was blockiert wurde, nach Standort und IP-Bereich. Zulassungs- und Sperrlisten passt EXYS auf Anfrage an.

RESOLVER 1. QUERY STREAM				TYPE	D
TIME	CLIENT	QUERY			
08:14:02.118	10.20.12.31	login.microsoftonline.com		A	1
08:14:02.164	10.20.12.31	outlook.office365.com		AAAA	1
08:14:02.390	10.20.14.7	cdn.jsdelivr.net		A	1
08:14:02.411	10.20.14.7	office365-mailbox-quota.site		A	1
08:14:02.733	10.20.12.58	www.admin.ch		A	
08:14:03.002	10.20.40.17	q7vk2x0pzt4rl.top		A	
08:14:03.019	10.20.40.17	h3m9wq1ckz8o.xyz		A	
08:14:03.044	10.20.40.17	z0rt6pl2vbn5yq.biz		A	
08:14:03.250	10.20.12.31	teams.microsoft.com		AAAA	
08:14:03.512	10.20.15.92	fonts.gstatic.com		A	
08:14:03.640	10.20.15.92	parcel-redelivery-ch.info		A	
08:14:03.871	10.20.21.4	time.windows.com		A	
08:14:04.106	10.20.12.58	www.sbb.ch		A	
08:14:04.322	10.20.30.12	update.googleapis.com		A	
08:14:04.380	10.20.30.12	invoice-docs-share.online		A	
08:14:04.517	10.20.14.7	api.github.com		A	
08:14:04.776	10.20.40.17	w4y8nq0t2jx6.click		A	
08:14:05.041	10.20.12.31	slack.com		A	
08:14:05.268	10.20.21.4	ocsp.digicert.com		AAAA	
08:14:05.390	10.20.15.92	www.linkedin.com		A	
08:14:05.611	10.20.12.58	secure-ebanking-ch-login.top		A	

WAS SIE BEKOMMEN:

- Resolver, gehostet und betrieben von EXYS in der Schweiz
- Schutz für jedes Gerät, das Namen abfragt, auch für unbeaufsichtigte IT- und OT-Geräte
- Sperre von Domains für Phishing, Betrug, Malware und Glücksspiel
- Machine Learning, das am Domainnamen selbst algorithmisch erzeugte, noch unbekannte Domains erkennt
- Tagesbericht per E-Mail und im Portal, mit Standorten und IP-Bereichen
- Mehr als 2,5 Millionen DNS-Anfragen pro Monat
- Nur die DNS-Einstellung ändern, nichts installieren
- Datenbank schädlicher Domains, täglich neu aufgebaut aus externen Feeds und eigenen Quellen von EXYS
- Keine Antwort auf blockierte Abfragen, damit Malware ihren Command-and-Control-Server nicht erreicht
- Zusätzlicher Abgleich mit der EXYS-Datenbank schädlicher IPs und URLs
- Optionale detaillierte Auswertung mit Risikoindikatoren und Empfehlungen

MIR SIND FÜR SIE DA.

ADRESSE

EXYS SA
Strada Regina 16
CH-6934 Bioggio
Tessin, Schweiz

KONTAKT

Telefon +41 (0)91 220 52 00

www.exys.swiss
office@exys.swiss

EXYS SA ist nach ISO/IEC 27001 zertifiziert



EXYS
WHERE PASSION
MEETS TECHNOLOGY

EXYS5100 - SECURE - DNS