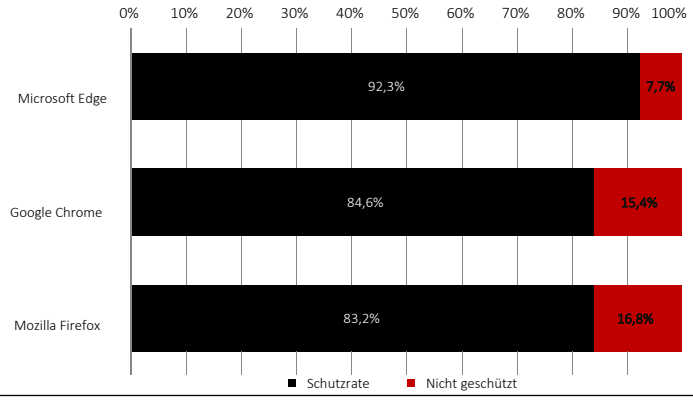
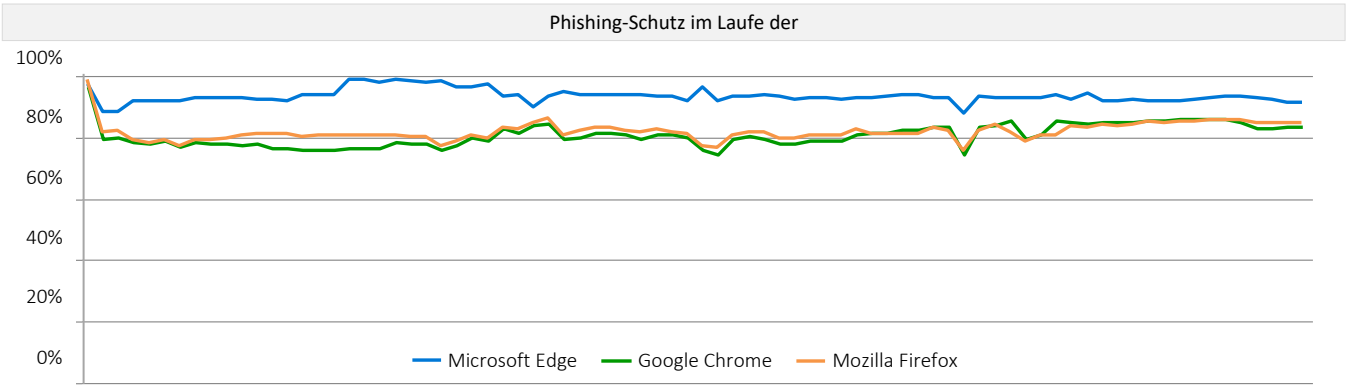
Q2 2021 Webbrowser vs. Phishing

Übersich

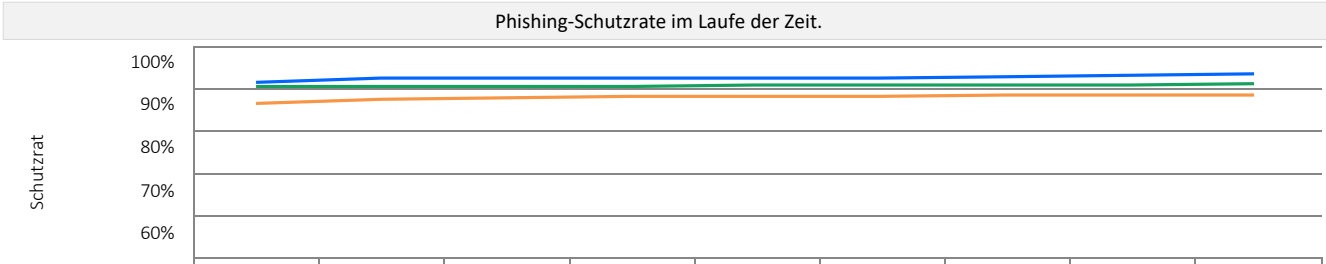
Im zweiten Quartal 2021 führte CyberRatings.org einen unabhängigen Test zum Thema "Schutz vor Phishing durch Webbrowser" durch. Die Tests liefen 20 Tage lang und umfassten 80 diskrete Testdurchläufe. Zum Schutz vor Phishing kommt bei Microsoft Edge der Microsoft Defender SmartScreen zum Einsatz; Google Chrome und Mozilla Firefox verwenden die Google Safe Browsing API. Microsoft Edge bot beim Test den höchsten Schutz, blockierte 92,3 % aller Phishing-URLs und bot gleichzeitig die höchste Zero-Hour-Schutzrate (93,5 %). Google Chrome bot mit durchschnittlich 84,6% den zweithöchsten Schutz, gefolgt von Mozilla Firefox mit 83,2%.



URL-Reputationssysteme verkürzen die Zeit von Angreifern, ihre Ziele zu erreichen, indem sie Anwender davor warnen, dass eine URL eine bekannte Phishing-Site ist. Da Anwender jedoch ein breites Spektrum an Websites besuchen, von denen viele zum ersten Mal besucht werden, können URL-Reputationssysteme nicht einfach alle neuen URLs sperren. Deshalb ändern sich Phishing-Kampagnen der Angreifer ständig, wobei der Großteil neuer Angriffe in den ersten Stunden nach Beginn des ersten Angriffs folgt.



Während des Tests wurden täglich neue Phishing-URLs hinzugefügt, und URLs, die entweder nicht mehr erreichbar waren oder keine Phishing-Angriffe mehr lieferten, wurden entfernt. Jeder Datenpunkt steht für den Schutz zu einem bestimmten Zeitpunkt. Wurde eine URL frühzeitig blockiert, bekam der Browser eine höhere Bewertung für konsistenten Schutz im Laufe der Zeit. Wenn der Browser die URL nicht blockierte, sank hingegen die Schutzbewertung.



Zusammenfassung

	0 Std.	1 Tag	2 Tage	3 Tage	4 Tage	5 Tage	6 Tage	7 Tage	Gesamt
Microsoft Edge	93,5%	94,4%	94,5%	94,5%	94,5%	94,7%	94,9%	95,1%	95,4%
Google Chrome	92,4%	92,6%	92,7%	92,7%	92,8%	92,8%	92,8%	92,9%	93,2%
Mozilla Firefox	88,7%	89,7%	90,0%	90,4%	90,4%	90,4%	90,5%	90,6%	90,6%

Wir haben die Fähigkeit des Browsers gemessen, schädliche URLs so schnell zu blockieren, wie sie auch im Internet entdeckt wurden. Das wurde alle sechs Stunden wiederholt, um festzustellen, wie lange ein Anbieter brauchen würde, den Schutz bereitzustellen. Die obige Abbildung zeigt die Reaktionszeit jedes einzelnen Browsers beim Blockieren einer Phishing-Site, nachdem die Bedrohung zum Testzyklus hinzugefügt wurde.

Phishing-Angriffe

Phishing ist eine Art Angriff durch soziale Manipulation, bei dem versucht wird, ein Opfer dazu zu bringen, dem Angreifer vertrauliche persönliche Informationen zu übermitteln. Einige Beispiele für vertrauliche Informationen sind Kreditkartennummern, Sozialversicherungsnummern sowie Anmeldedaten und Kennwörter für Bankkonten. E-Mails, Sofortnachrichten, SMS-Nachrichten und Links in sozialen Netzwerken sind allesamt anfällig für Phishing-Angriffe. Die Zielseite einer Phishing-Website versucht oft, den Computer eines Besuchers unbemerkt auszunutzen und schädliche Software zu installieren (ein so genannter Drive-by-Exploit).

Phishing-Angriffe stellen ein erhebliches Risiko für Einzelpersonen und Unternehmen dar, da sie damit drohen, vertrauliche persönliche und Unternehmensdaten zu gefährden oder zu erlangen. Die Anti-Phishing Working Group (APWG) meldete im vierten Quartal 2020 insgesamt 396.688 einzigartige E-Mail-Phishing-Kampagnen.[1]

Phishing-Schutz durch Webbrowser

Phishing-Schutz wird durch eine Anwendung von Webbrowsern bereitgestellt, die die Reputation einer URL von einem Clouddienst abfragt, der das Internet nach Phishing-Websites durchsucht und sie zu einer Blockierliste hinzufügt. Wenn ein Webbrowser versucht, eine URL aufzurufen, zeigt der Phishing-Schutz des Browsers (d. h. Safe Browsing, SmartScreen usw.) dem Anwender eine Warnmeldung an, die erklärt, dass die URL schädlich ist. Manche Reputationssysteme beinhalten auch zusätzliche Informationsangebote. Wird eine Website hingegen als „gut“ eingestuft, macht der Webbrowser nichts.

Google und Mozilla verwenden die Google Safe Browsing API für die URL-Reputation, zum Warnen von Anwendern vor dem Herunterladen bestimmter Dateitypen oder zum Blockieren dieser Dateitypen. Bei Microsoft Edge kommt Microsoft Defender SmartScreen zum Einsatz, der URL-basierten Schutz vor Angriffen über einen integrierten, cloudbasierten URL-Reputationsdienst sowie eine Anwendungsreputation zum Blockieren schädlicher Dateien bietet.

Durchschnittliche Anzahl der täglich hinzugefügten URLs

Im Durchschnitt wurden pro Tag 50 neue validierte URLs zum Testsatz hinzugefügt; an manchen Tagen schwankte die Zahl, da nicht jeden Tag gleich viele kriminelle Aktivitäten auftraten.

Testumgebung

- Microsoft Windows 10 Pro, 21H1

Gesamtzahl schädlicher URLs im Test

26.976 rohe, nicht validierte URLs wurden bei jedem Webbrowser mehrfach getestet in insgesamt 80 Testzyklen, die ohne Unterbrechung über 480 Stunden (alle 6 Stunden über 20 Tage) durchgeführt wurden. Unsere Techniker entfernten Muster, die die Validierungskriterien nicht erfüllten, einschließlich solcher, die durch Exploits unbrauchbar waren (nicht Teil des Tests). Letztendlich wurden 996 eindeutige, gültige Phishing-URLs in den endgültigen Satz von 61.605 diskreten, gültigen Phishing-Tests (20.535 Tests pro Webbrowser) aufgenommen, was eine Fehlermarge von weniger als 3,1 Prozent (3,1%) bei einem Konfidenzniveau von 95 % ergibt.

Testzusammenstellung – Phishing-URLs

Die Daten in diesem Test beziehen sich auf einen Testzeitraum von zwanzig (20) Tagen zwischen 11. und 31. Mai 2021. Während des Tests überwachten unsere Techniker routinemäßig die Konnektivität, um sicherzustellen, dass die getesteten Browser auf Phishing-URLs als auch auf Browser-Reputationsdienste in der Cloud zugreifen konnten.

Der Schwerpunkt lag auf Aktualität der URLs, wobei ständig neue URLs in den Test aufgenommen und tote Sites entfernt wurden.

Wie wir die Ergebnisse bewertet haben

Wir haben die Fähigkeit der einzelnen Browser gemessen, schädliche URLs so schnell zu blockieren, wie sie auch im Internet entdeckt wurden. Die Techniker wiederholten die Tests alle sechs Stunden, um festzustellen, wie lange ein Anbieter brauchte, den Schutz bereitzustellen oder ob er es überhaupt tat.

Die Leistung aller Browser wurde kontinuierlich gemessen, und die Gesamtschutzrate aller mit den Browsern getesteten URLs wurde aufgezeichnet. Die Gesamtschutzrate jedes Browsers wurde berechnet als die Anzahl der erfolgreichen Blockierungen geteilt durch die Gesamtzahl der Testfälle. Wenn beispielsweise alle 6 Stunden Tests durchgeführt werden, wurde ein URL, die 48 Stunden lang online war, acht (8) Mal getestet. Ein Browser, der es bei 6 (von maximal 8) Testläufen blockierte, erreichte eine Schutzrate von 75 %.

Getestete Produkte

- Google Chrome: Version 90.0.4430.212 - 91.0.4472.19
- Microsoft Edge: Version: 91.0.864.19 - 91.0.864.37
- Mozilla Firefox: Version 88.0.1 - 88.0.1

[1] APWG-Trendbericht zu Phishing-Aktivitäten

Autoren

Thomas Skybakmoen, Vikram Phatak

Testmethodik

CyberRatings Webbrowser-Sicherheitstestmethodik v1.0 ist verfügbar unter www.cyberratings.org

Kontaktinformationen

CyberRatings.org
2303 Ranch Road 620 South
Suite 160, #501
Austin, TX 78734

info@cyberratings.org
www.cyberratings.org