

Link: <https://www.computerwoche.de/a/spionage-warum-nicht,2351357>

Sophos-Studie über Cyberkriminalität

Spionage - warum nicht?

Datum: 16.08.2010
Autor(en):Ima Buxton

Dass das Internet Cyberkriminellen als Plattform für die eigene finanzielle Bereicherung dient, ist längst bekannt. Einer aktuellen Sophos-Studie zufolge entwickelt sich im Web aber bereits ein Krieg um die Vormachtstellung einzelner Länder und Personengruppen.

□

Foto:

Unternehmen weltweit erachten den Einsatz cyberkrimineller Aktivitäten als eine für ihr Land vertretbare Methode der Spionage. Wie eine Umfrage des **Security**¹-Spezialisten Sophos enthüllt, akzeptieren 63 Prozent der Befragten Landesspionage via Internet. Rund ein Drittel befürwortete, dass Länder die Erlaubnis haben sollten, private ausländische Unternehmen mittels Hacking und **Malware**² ausspionieren zu dürfen. "Es ist überraschend, dass so viele Befragte es akzeptieren, dass das Internet zu Spionagezwecken oder gar als Waffe genutzt wird", sagt Graham Cluley, Senior Technology Consultant von Sophos und mahnt zugleich: "Doch grünes Licht für derartige Web-Aktivitäten zu geben, bedeutet auch, dass man selbst eines Tages Opfer eines Spionageangriffes werden könnte."

Sophos befragte für seine Erhebung mehr als 1077 Unternehmen. Einer von 14 Befragten vertrat dabei die Auffassung, dass Denial-of-Service-Attacken gegen die **Kommunikation**³ anderer Länder oder Finanzwebseiten vertretbar sind. 32 Prozent befürworteten klar, Schadprogramme gegen private Unternehmen mit dem Ziel einzusetzen, **wirtschaftliches Know-how**⁴ abzugreifen.

Zunehmende Cyber-Attacken auf soziale Netzwerke

Die Halbjahresbilanz des aktuellen Sophos Threat Reports bestätigt zudem den zunehmenden Trend von Cyber-**Attacken auf Mitglieder**⁵ **sozialer Netzwerke**⁶ in Form von Schadprogrammen. Inzwischen sind mehr europäische Länder wie Frankreich, Italien und Holland in die Top-Ten der Länder aufgerückt, die die meisten Webseiten mit Schadprogrammen hosten. Deutschland nimmt Rang vier ein.

"Es entwickelt sich eine organisierte Kriminalität"

"Hacking und die Entwicklung von **Virenprogrammen**⁷ waren früher oft ‚nur‘ Hobby, mit dem Ziel, die Intelligenz der Programmierer auf den Prüfstand zu stellen und nicht, um dauerhaften Schaden anzurichten", kommentiert Cluley die Ergebnisse. "Doch langsam entwickelt sich daraus eine organisierte Kriminalität, bei der es um viel Geld geht. Aktuell könnte man eine dritte Motivation in den Raum stellen: **Cyberkriminelle**⁸ setzen Malware ein, um einen wirtschaftlichen, politischen und auch militärischen Vorteil über andere Länder oder Personen zu gewinnen."

Links im Artikel:

¹ <https://www.computerwoche.de/security/2349551/>

² <https://www.computerwoche.de/fileserver/idgwpcw/files/1778.pdf>

-

- 3 <https://www.computerwoche.de/filesserver/idgwpcw/files/1779.pdf>**
 - 4 <https://www.computerwoche.de/filesserver/idgwpcw/files/1770.pdf>**
 - 5 <https://www.computerwoche.de/subnet/telekom/mobilitaet/2350579/>**
 - 6 <https://www.computerwoche.de/filesserver/idgwpcw/files/1760.pdf>**
 - 7 <https://www.computerwoche.de/netzwerke/mobile-wireless/2350104/>**
 - 8 <https://www.computerwoche.de/security/2350082/>**
-

IDG Tech Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.