



# Was ist eine Sandbox?

E-Book zum Thema Sandbox-Lösungen und welchen Nutzen sie für Firmen haben.

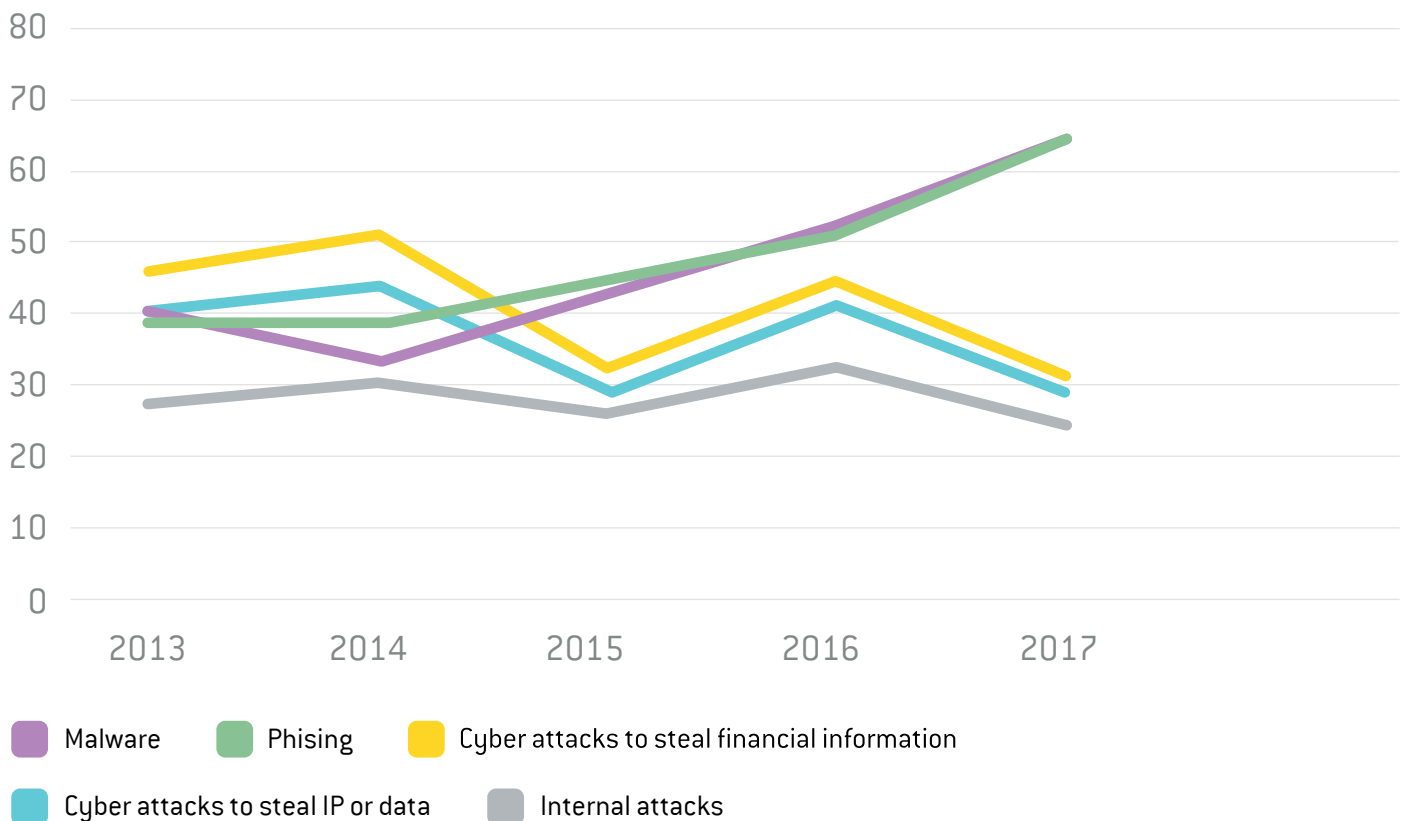
# Bedrohungslage

Die Häufigkeit, die Komplexität und der Umfang von Cyberangriffen nehmen laufend zu, ebenso die Ausbreitungsgeschwindigkeit der Schadsoftware.

Deren Entwickler nutzen neue, noch unbekannte Schwachstellen und kennen die meisten Sicherheitstechnologien. Daher setzen sie Tarnungen und ausgeklügelte Verschleierungsmethoden ein.

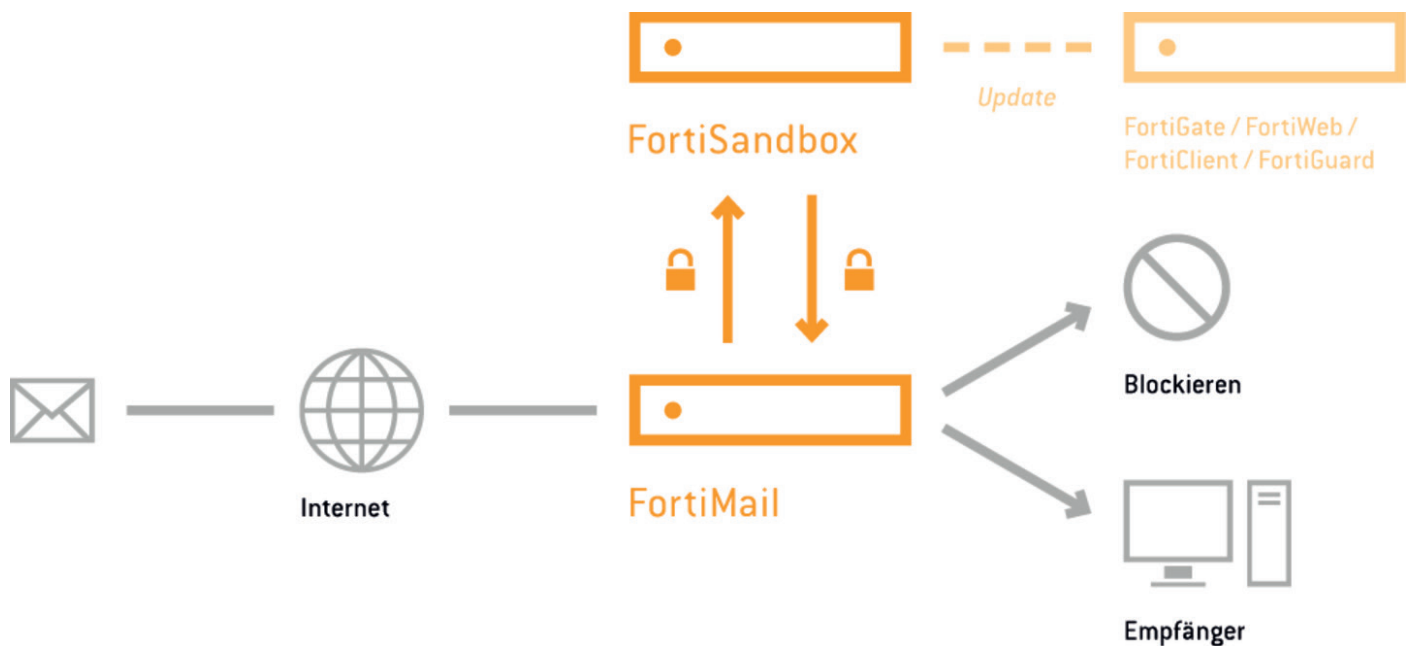
**90 Prozent** der erfolgreichen Cyberangriffe gelangen per E-Mail-Anhang, über schädliche Links oder infizierte Webseiten auf die Systeme.

% of respondents stating as top two items to increase risk exposure



Data Source: helpnetsecurity.com

# Erkennung hochentwickelter Malware



Mit der Sandbox-Technologie werden verdächtige Dateien und URLs in einer isolierten Umgebung ausgeführt. Das Verhalten wird in der abgesicherten Umgebung analysiert und schädliches Verhalten wird erkannt.

Die Hashwerte bössartiger Dateien oder als bössartig erkannte URLs werden gespeichert und können auf alle Sicherheitskomponenten der Infrastruktur verteilt werden. Bereits geprüfte Dateien oder URLs werden erkannt und müssen nicht ein zweites mal in der Sandbox getestet werden.

# Gemeinsam gegen Malware

Bei neuen Bedrohungen dauert es oft einige Zeit, bis neue Updates für die Erkennungsmechanismen verfügbar sind. Während dieser Zeit sind die Systeme ungeschützt und ein leichtes Ziel für neue Malware. Sandbox-Lösungen erkennen Malware welche traditionelle Security-Lösungen umgehen können und für die noch keine Signaturen vorhanden sind.

Sandbox-Lösungen verhindern auch Zero-Day-Exploit's. Das sind Angriffe auf ein System, die eine unbekannte Schwachstelle ausnutzen. Entwickler hatten dadurch keine Zeit („null Tage“), die Software so zu verbessern, so dass der Exploit unwirksam wird. Mit Hilfe eines Exploits wird sich Zugang zum System eines Opfers verschafft, um daraufhin ein Schadprogramm (Malware) einzuschleusen. Bekannte Arten von Malware sind Viren, Würmer, Trojaner, Spyware, oder Ransomware.



## Vom Experten beraten lassen

Unser Consulting-Team steht Ihnen für weitere Auskünfte gerne zur Verfügung.

Sie erreichen uns über [verkauf@firstframe.net](mailto:verkauf@firstframe.net) oder +41 41 768 08 00.

first frame networkers ag  
haldenstrasse 1  
ch-6340 baar

[www.firstframe.net](http://www.firstframe.net)  
[info@firstframe.net](mailto:info@firstframe.net)  
+41 41 768 08 00