EIN LEICHT VERSTÄNDLICHER LEITFADEN ZU

GROSSANGRIFFEN, FORTSCHRITTLICHEN CYBERGEFAHREN UND GEZIELTEN ANGRIFFEN

F-Secure.

GROSSANGRIFFE KOMMEN AM HÄUFIGSTEN VOR – GEZIELTE ANGRIFFE MACHEN DEN GRÖSSTEN SCHADEN

GROSS ANGRIFFE

Massenhafte
Malware
Phishing
Spam
Online Scams

FORTSCHRITTLICHE GEFAHREN

Fileless
Zero-Day
Exploits
Ransomware

GEZIELTE ANGRIFFE

System-Tools
Gezieltes Phishing
Social Engineering
Individualisierte
Malware

GROSSANGRIFFE WERDEN DURCH MASCHINEN DURCHGEFÜHRT

FORTSCHRITTLICHE & GEZIELTE ATTACKEN

BENÖTIGEN HOCHQUALIFIZIERTE MENSCHLICHE ANGREIFER

>100 MILLIONEN
neue Malware-Samples jedes Jahr
(AV-TEST Database)

35%
der Angriffe im Jahr 2018 werden Fileless Attacken sein
(2017 State of Endpoint Security Risk, Ponemon Institute & Barkly, November 2017)

Fileless Attacken sind fast

10×
erfolgreicher als traditionelle Datei-basierte Attacken
(2017 State of Endpoint Security Risk, Ponemon Institute & Barkly, November 2017)

72%
aller Unternehmen waren von Phishing betroffen, was ebenfalls die größten Auswirkungen auf die Unternehmen hatte
(2017 Threat Landscape Survey: Users on the Front Line, SANS Institute, August 2017)

ALLGEMEINE GEFAHREN
Können durch Endpoint Protection, Firewalls und andere präventive Maßnahmen verhindert werden

FORTSCHRITTLICHE UND GEZIELTE CYBERATTACKEN
sind am gefährlichsten und können n
durch Lösungen zur Erkennung und A
begegnet werden

99.9%
verursachen kaum Schäden

0.1%
verursachen die größten Schäden

ALLGEMEINE GEFAHREN | GEZIELTE ATTACKEN

UNTERNEHMEN VERSTEHEN DIE NOTWENDIGKEIT SICH AUF ATTACKEN ZU FOKUSSIEREN, DIE DIE STANDARDABWEHR UMGEHEN KÖNNEN

DIE TOP 3 SICHERHEITSPRIORITÄTEN FÜR UNTERNEHMEN

Verhindern von Datenlecks und dem Verlust von Kunden- oder Unternehmensdaten/IP — 36%

Sicherstellung des Schutzes vor Malware und Ransomware — 34%

Entdeckung von Angriffen, die andere Sicherheitsmaßnahmen überwunden haben könnten — 31%

* Quelle: F-Secure Security Priorities of Companies 2017 Report

WELCHE TAKTIKEN NUTZEN DIE ANGREIFER?

62% der Angriffe nutzten Hacking

51% der Angriffe nutzten Malware

* Quelle: Verizon, 2017 Data Breach Investigations Report

WIE VERHALTEN SICH DIE ANGREIFER NACH DEM EINBRUCH?

57%
VERHIELTEN SICH WIE EIN STANDARD USER

43%
ZEIGTEN SCHÄDLICHES VERHALTEN

Quelle: F-Secure Threat Landscape H1 2017 Report

EINE KOMBINATION VON MENSCH UND MASCHINE IST NOTWENDIG, UM EINEN EINBRUCH ZU ERKENNEN

Smart Software und Machine Learning filtern die offensichtlichen Fälle

Menschliche Experten analysieren die Anomalien

2 MILLIARDEN **Daten-Events / Monat**
gesammelt von ~1000 Endpunktsensoren

900 000 **verdächtige Vorfälle**
nach Echtzeitanalyse des Verhaltens

25 **Erkennungen**
nach Erweiterung des Kontext der verdächtigen Vorfälle

15 **echte Gefahren**
nach der Bestätigung der Erkennungen als echte Gefahren

UNTERNEHMEN FEHLEN EIGENE CYBERSECURITY EXPERTEN

1,5 MILLIONEN Frost & Sullivan sagen ein Fehlen von 1,5 Millionen Cybersecurity Experten bis 2020 voraus.

Eins von vier Unternehmen sieht sich bereits jetzt einem "problematischen Mangel" an Experten gegenüber.

DURCHSCHNITTSKOSTEN EINES VORFALLS?

$3,62 MIO.

Quelle: IBM & Ponemon Institute Cost of Data Breach Study 2017

WARUM SICH AUF SCHÄTZUNGEN VERLASSEN? MAN KANN REALISTISCHE ZAHLEN ZUR EVALUIERUNG DER CYBERRISIKEN ANLEGEN

Wie? Das sehen Sie auf de.business.f-secure.com

WIE KANN MAN SICH ABSICHERN?

Stärken Sie Ihre Basissicherheit mit präventiver Sicherheit, aber vergessen Sie weitere Lösungen zur Erkennung und Abwehr nicht

MANAGED DETECTION & RESPONSE (MDR)

ENDPOINT DETECTION & RESPONSE (EDR)

INCIDENT RESPONSE SERVICES

F-Secure.