Der Faktor Mensch

proofpoint.

Cybersicherheit, Ransomware und E-Mail-Betrug in einem Jahr, das die Welt veränderte

Während die weltweite Pandemie die beruflichen und privaten Abläufe auf den Kopf stellte, sahen die Cyberangreifer ihre Chance gekommen. Und jetzt, im Jahr 2021, beobachten wir, wie Cyberkriminelle ihre Vorteile voll ausnutzen.

Personenzentrierte Angriffe erfordern personenzentrierte Schutzmaßnahmen, die die drei grundlegenden Facetten von Cybersicherheitsrisiken berücksichtigen.

Schwachstellen

Wie wahrscheinlich ist es, dass Ihre Anwender Opfer eines Cyberangriffs werden?

20 %

der Anwender bestehen Cyberbedrohungstests **mit Anhängen** nicht.

Zu diesen Anhängen gehören schädliche Dateien.

12 %

der Anwender bestehen Cyberbedrohungstests **mit Links** nicht.

Zu diesen Links gehören gefährliche URLs, die zu Malware und schädlichen Websites führen.

4 %

der Anwender bestehen Cyberbedrohungstests **mit Dateneingabe** nicht.

Dabei werden die Anwender zu einer gefälschten Anmeldeseite geführt, die Anmeldedaten und andere personenbezogene Daten stehlen soll.

Einige der erfolgreichsten Angriffstechniken des Jahres 2020 waren äußerst gezielt und wurden in Kampagnen eingesetzt, die manchmal nur eine Handvoll E-Mails umfassten.

Steganografie bezeichnet das Verbergen von schädlichem Code in Bildern und anderen Dateitypen. Mehr als **30 % der Anwender** klickten auf eine schädliche E-Mail mit Steganografie-Daten.

CAPTCHA-Techniken verwenden visuelle Puzzles zur Unterscheidung von Menschen und Maschinen. Die Klickraten sind im Jahresvergleich **um das 50-fache gestiegen**.

Angriffe

Welchen Arten von Bedrohungen sind Ihre Anwender ausgesetzt?

Die Pandemie war 2020 der wichtigste Köder. Fast jeder Bedrohungsakteur nutzte mindestens einmal Inhalte mit COVID-Bezug.

Unabhängig vom Köder variierten die Angriffsmethoden:

Anmeldedaten-Phishing machte fast **zwei Drittel** der schädlichen Nachrichten aus.

25 % der Angriffskampagnen versteckten Malware in komprimierten ausführbaren Dateien.

10 % aller schädlichen Kampagnen-E-Mails versuchten, Emotet-Malware zu verteilen.

Remote-Zugriffs-Trojaner kamen in fast **25 % aller E-Mail**-Bedrohungskampagnen zum Einsatz.

Mehr als 48 Mio. Nachrichten enthielten Malware, die als Einstiegspunkt für Ransomware-Angriffe dienen konnte.

10-fach
Zunahme bei Excel 4.0-Makro-Angriffen

5-fach
Zunahme bei Angriffen mit kennwortgeschützten Dateien

18 %
Zunahme bei Thread-Hijacking-Angriffen

2019 und 2020 im Vergleich

Berechtigungen

Wie groß ist das Schadenspotenzial eines Angriffs?

Je umfangreicher die Berechtigungen eines kompromittierten Kontos, desto mehr vertrauliche und wertvolle Daten sind bei unbefugten Zugriffen gefährdet und desto größer sind die Auswirkungen eines Cyberangriffs.

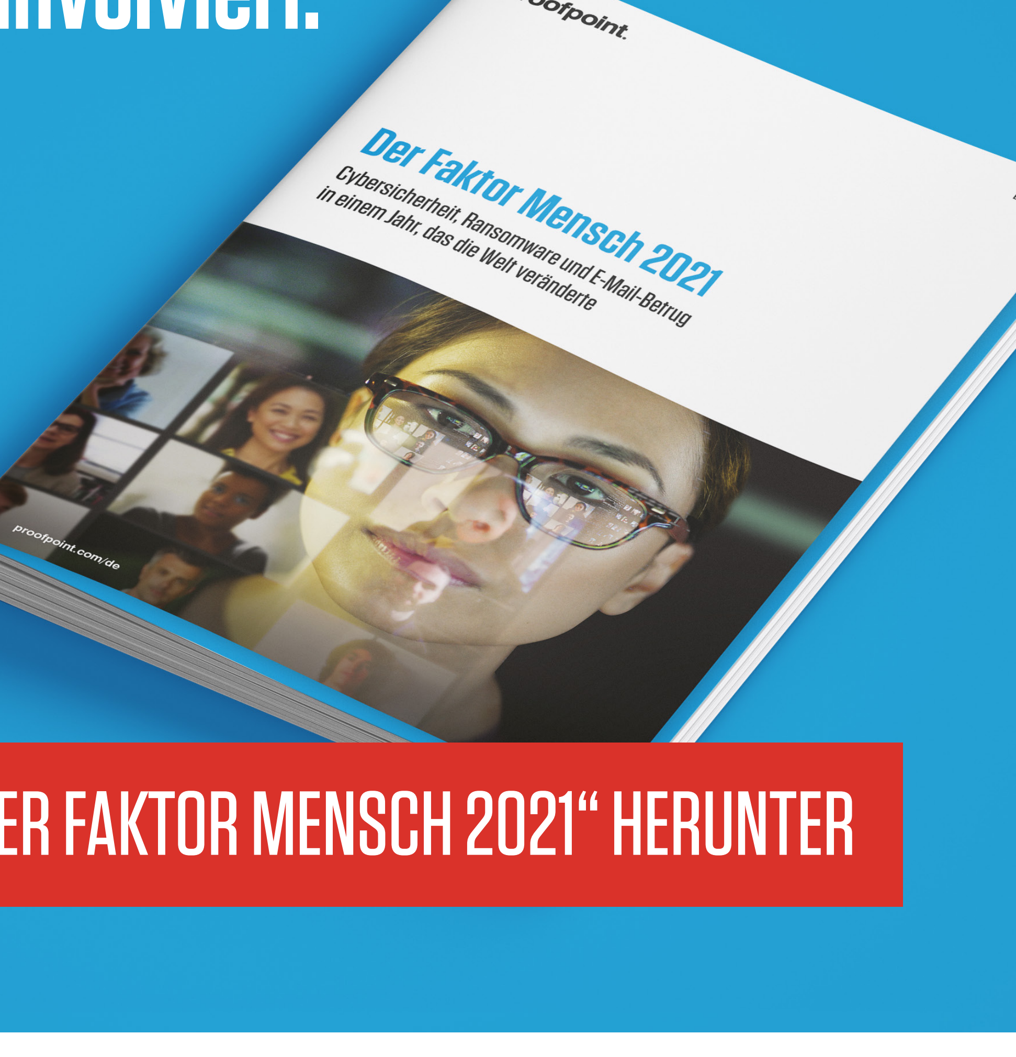
Der Wechsel zu hybriden und Remote-Arbeitsplätzen steigert das Risiko von Bedrohungen durch böswillige oder fahrlässig handelnde Insider.

Häufigste Warnungen bei der Abwehr von Insider-Bedrohungen:

- ⚠ Anschließen eines nicht gelisteten USB-Geräts
- ⚠ Exfiltrieren einer überwachten Datei ins Internet per Upload
- ⚠ Öffnen einer Klartextdatei, die Kennwörter enthalten könnte
- ⚠ Herunterladen von Dateien mit potenziell schädlichen Erweiterungen
- ⚠ Kopieren großer Dateien oder Ordner außerhalb der üblichen Zeiten
- ⚠ Exfiltrieren einer Datei auf nicht gelistetes USB-Gerät
- ⚠ Installation von Hacker- oder Spoofing-Tools
- ⚠ Zugriff auf Cloud-Dienste für Upload und Freigabe

Die Lösung des Problems „Faktor Mensch"

Cyberangriffe lassen sich nicht vermeiden. Fast immer ist jedoch ein Mensch involviert.



Bereiten Sie Ihre Mitarbeiter mit Schulungen zur Sensibilisierung für Sicherheit und mit risikobasierten Kontrollen darauf vor, Ihr Unternehmen zu schützen. Informieren Sie sich...

LADEN SIE DEN BERICHT „DER FAKTOR MENSCH 2021" HERUNTER

Weitere Informationen finden Sie unter proofpoint.com/de.

proofpoint.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.