

# DER FAKTOR MENSCH 2017

Böswillige E-Mail-Angriffe nutzen Menschen aus – und nicht Code.

Dies sind die Techniken, mit denen Cyberkriminelle im Jahr 2016 am häufigsten Benutzer zum Öffnen böswilliger E-Mails und Social-Media-Beiträge verleiteten.



## BEC-ANGRIFFE (BUSINESS EMAIL COMPROMISE) NEHMEN ZU

Das Volumen der BEC-Nachrichten stieg von 1% im Jahr 2015 auf **42% zum Ende 2016**.



## SOCIAL-MEDIA-KONTO-PHISHING WIRD IMMER BELIEBTER

Social-Media-Phishing nahm im Jahr 2016 **um 150%** zu.



## MALWARE-KATEGORIEN VARIIEREN IHRE VERBREITUNG VON TAG ZU TAG

Ransomware-Kampagnen werden bevorzugt von **Dienstag bis Donnerstag** durchgeführt.



## ZEIT IST GELD

**87%** aller Klicks auf böswillige URLs finden innerhalb der ersten 24 Stunden nach Eingang statt.



Fast 50% der Klicks erfolgen innerhalb einer Stunde.



25% aller Klicks erfolgen innerhalb von nur 10 Minuten.

## ANGRIFFSSPITZE IST UM DIE MITTAGSZEIT

Klicks erreichen ihren **Höchstwert 4 bis 5 Stunden** nach Arbeitsbeginn, also um die Mittagszeit.



## BETRÜGERISCHE MOBILGERÄTE-APPS LEGEN BENUTZER HEREIN

Böswillige Apps **missbrauchen Marken und nutzen irreführende Namen**, um Benutzer zum Download der Malware zu verleiten.



## MEHR MOBILTELEFONE BEDEUTEN MEHR RISIKEN

42% aller Klicks auf böswillige URLs erfolgen auf Mobilgeräten – **zweimal mehr als die 20% im Vorjahr**.



LADEN SIE DEN VOLLSTÄNDIGEN BERICHT HERUNTER  
[proofpoint.com/de/human-factor-report-2017](http://proofpoint.com/de/human-factor-report-2017)