

Gruselgeschichten des Netzes

Die gespenstischsten Sicherheitsrisiken und schrecklich wirksame Schutzmaßnahmen



Grusel im Web gibt es nicht nur zu Halloween.

Zur schaurigsten Nacht des Jahres stellt DomainFactory die finstersten Cyber-Geister und wichtigsten Schutzmaßnahmen vor – damit auf das süße Netzerlebnis nicht ein saures Erwachen folgt.

Erschreckende 47 % der deutschen Internetnutzer sind im letzten Jahr Opfer von Cybercrime geworden.¹ Hier die Netz-Ungeheuer, die den größten Schrecken verbreiten:

Distributed Denial of Service (DDoS)

Gekaperte Rechner IoT-Geräte werden als sogenannte Zombies in einem Bot-Netzwerk zusammengefasst. 80 % der verkauften IoT-Geräte besitzen unsichere Passwörter und sind daher einfache Opfer.²

Das französische Unternehmen OVH wurde Opfer einer **1 TBit/s** Attacke, die über **150.000** gehackte IoT-Devices gesteuert wurde.⁴

620 GBit/s an Datenmüll prasselten auf die Website des Journalisten Brian Krebs ein.³

In die kürzliche Attacke auf Dyn waren mehr als **10 Millionen** IP-Adressen involviert, darunter zahlreiche IoT-Devices.⁵

Die längste Attacke dauerte **15,5 Tage**.⁶

Vor der Wahl des Hosting-Partners sollten Sie informieren, welche Schutzmaßnahmen dieser bietet: z.B. Schutz-Algorithmen, die auffällige Muster erkennen und schlechten Traffic blocken und ein Team, das bei Bedarf steuernd eingreifen kann.

Malware und Ransomware

Im Frühjahr 2016 identifizierten Virenschutzprogramme ca. **1.100 %** mehr Ransomware in Deutschland.⁷

Ob Virus, Trojaner oder Verschlüsselungswurm: **430+ Millionen** Varianten sind 2015 neu entdeckt worden.⁸

Es ist ungeheuer wichtig, dass Ihre Virenschutzsoftware auf dem neusten Stand ist. Und machen Sie regelmäßig Backups, um im Notfall eine Sicherung einspielen zu können.

Hacks und Diebstahl

469 Tage brauchen europäische Unternehmen, um einen Hack zu entdecken...

...und durchschnittlich wurden nachweisbare **2,6 GB** an Daten gestohlen!⁹

Verschlüsseln Sie Ihre Daten! Dann haben Datendiebe kaum eine Möglichkeit, auf die gestohlenen Daten zuzugreifen.

Spam und Phishing

Über **50 %** des E-Mail Traffics sind Spam-Mails und führen ihre Empfänger oftmals auf gefälschte Webseiten. Vor allem auf Online-Shops, um Nutzer- und Bankdaten zu erbeuten.¹⁰

Top 5 der Phishing-Ziele:¹⁰

Apple **27,82 %**

Amazon **21,60 %**

Steam **13,23 %**

Alibaba **6,05 %**

eBay **6,15 %**

Benutzer:

Passwort:

Kein Hexenwerk: Seiten, über die sensible Daten übermittelt und Geschäfte abgewickelt werden, niemals aus einer E-Mail öffnen, sondern immer direkt im Browser eingeben. Prüfen Sie auch, ob die Seite über <https://> erreichbar ist.

Quellen:

- <https://www.bitkom.org/Presse/Presseinformation/Jeder-zweite-Internetnutzer-Opfer-von-Cybercrime.html>
- <https://www.hpe.com/h20195/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en>
- <https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/>
- <http://securityaffairs.co/wordpress/51726/cyber-crime/ovh-hit-botnet-iot.html>
- http://www.kaspersky.com/de/about/news/virus/2016/Langster_DDoS-Angriff_2015_dauerte_15_5_Tage
- <http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/>
- <https://resource.elq.symantec.com/istr-vol21-de>
- https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/Ransomware.pdf?__blob=publicationFile&v=3
- <https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf>
- <https://de.securelist.com/analysis/quartalsreport-spam/71429/spam-and-phishing-in-q1-2016/>