

[HOME \(/\)](#) [COLLECTIONS \(/COLLECTION\)](#) [MAGAZIN \(/MAGAZIN\)](#) [SERIEN \(/VIDEO/SERIEN\)](#)[MEMBERSHIP \(HTTPS://MEMBERSHIP.WIRED.DE\)](https://MEMBERSHIP.WIRED.DE) [CAMPUS \(HTTPS://CAMPUS.WIRED.DE\)](https://CAMPUS.WIRED.DE)[NEWSLETTER \(HTTP://NEWSLETTER.WIRED.DE\)](http://NEWSLETTER.WIRED.DE)[f \(https://www.facebook.com/WIREDGermany\)](https://www.facebook.com/WIREDGermany) [t \(https://twitter.com/WIRED_Germany\)](https://twitter.com/WIRED_Germany)[i \(https://www.instagram.com/wiredgermany/\)](https://www.instagram.com/wiredgermany/)[You Tube \(https://www.youtube.com/user/WIREDde\)](https://www.youtube.com/user/WIREDde)[X \(https://www.xing.com/news/pages/wired-germany-79\)](https://www.xing.com/news/pages/wired-germany-79)

WIRED

Tech

Business

Gadgets


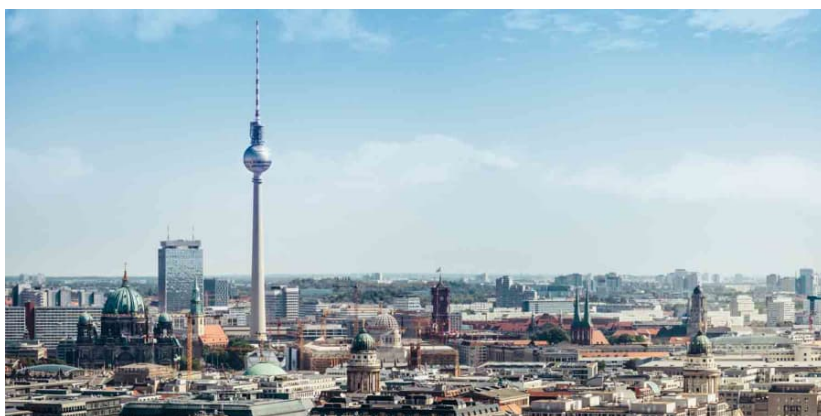
Life 

Science

Design

[\(/\)](#)[\(/Collection/](#)[Collection/](#)[Collection/](#)[Collection/](#)[Collection/](#)[Collection/](#)[/tech\)](#)[/business\)](#)[/gadgets\)](#)[/life\)](#)[\(https://membersh](#)[ip.wired.de](#)[/?promo=header_shopbutton\)](#)[/TECH \(/COLLECTION/TECH\)](#)

Wie die Ransomware-Attacke ein Berliner Startup weltbekannt machte

 Benedikt Plass-Fleßenkämper 28.06.2017

Getty Images

WIRED Newsletter

Regelmäßig neue Updates
aus dem WIRED-Kosmos!

[ANMELDEN \(HTTP://NEWSLETTER.WIRED.DE\)](http://newsletter.wired.de)

Das Startup Posteo aus Berlin kam über Nacht in die Schlagzeilen, weil der deutsche E-Mail-Anbieter das

Postfach der Petya-Erpresser umgehend löschte. WIRED erklärt, wer hinter dem jungen Unternehmen steckt und was es so besonders macht.

Seit dem 27. Juni wütet wieder eine globale Ransomware-Attacke (<https://www.wired.de/collection/tech/petrwap-wannacry-ransomware>): Petya – auch Petrwrap genannt – nutzt die gleichen Lücken wie WannaCry (<https://www.wired.de/collection/life/wannacry-hackerangriff-ransomware-deutsche-bahn>) aus und befahl die Computersysteme zahlreicher Unternehmen. Zu den Betroffenen gehören unter anderem der Pharmakonzern Merck, der Konsumgüterproduzent Beiersdorf (<http://www.ndr.de/nachrichten/hamburg/Computerattacke-trifft-wohl-auch-Beiersdorf-beiersdorf226.html>), das Logistikunternehmen Maersk (<https://twitter.com/Maersk/status/879675963927351296>), der Lebensmittelkonzern Mondelez (<http://www.mondelezinternational.com/newsroom/our-stories/Media-Statement-Global-Outage>) International und das Kernkraftwerk in Tschernobyl (<http://www.manager-magazin.de/unternehmen/artikel/hacker-angriff-cyber-attacke-trifft-auch-maersk-saint-gobain-und-wpp-a-1154749.html>).

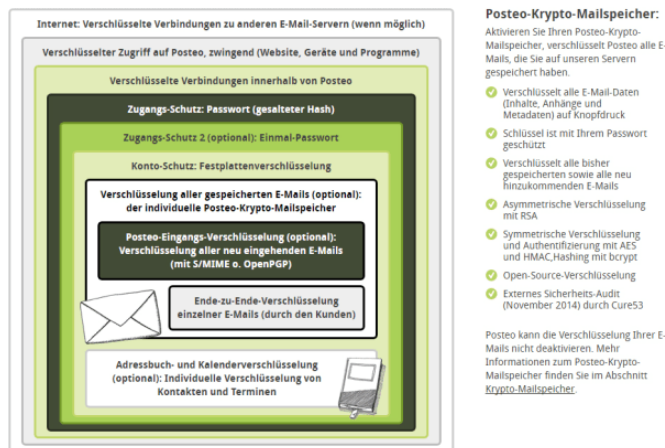
Petya gelangt über eine Windows-

Sicherheitslücke auf die Rechner, danach booten diese neu und auf dem Bildschirm erscheint eine Lösegeldforderung (<http://www.it-zoom.de/it-director/e/petya-greit-an-17111/>). Die betroffenen Unternehmen sollen 300 US-Dollar (rund 265 Euro) überweisen, damit ihre Computer wieder entsperrt werden – das zumindest versprechen die Erpresser. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) riet von Anfang an, auf die Lösegeldforderungen nicht einzugehen (https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/PM_petya_global_27062017.html;jsessionid=E0BFFFBB234BEDF92275BEC5D42). Mittlerweile ist dieser Hinweis doppelt so wichtig: Einerseits, weil die Erpresser in ihren Machenschaften nicht unterstützt werden dürfen. Andererseits, weil die angegebene Mailadresse gesperrt wurde. Dementsprechend können die Cyberkriminellen nicht mehr kontaktiert (https://motherboard.vice.com/en_us/article/new8xw/hacker-behind-massive-ransomware-outbreak-cant-get-emails-from-victims-who-paid) werden.

Die Mailadresse lag beim deutschen Anbieter Posteo (https://posteo.de/site/ueber_posteo), der durch Petya nun weltweit bekannt wurde. Nachdem das Berliner Startup am 27. Juni erfuhr, dass bei der Lösegeldforderung eine Posteo-Adresse angegeben wird, sperrte es umgehend (<https://posteo.de/blog/info-zur-ransomware-petrwrappetya-betroffenes-postfach-bereits-seit-mittag-gesperrt>) das entsprechende Postfach – was allerdings nicht von allen Sicherheitsexperten begrüßt wurde.

Als Begründung für diese Maßnahme gibt Posteo an: „Wir dulden keinen Missbrauch unserer Plattform: Das umgehende Sperren missbräuchlich genutzter Postfächer ist ein übliches Vorgehen von Providern in solchen Fällen.“

Doch wer ist Posteo überhaupt? Das junge Unternehmen bezeichnet sich selbst als „unabhängiger deutscher E-Mail-Anbieter“, der „großen Wert auf Nachhaltigkeit, Sicherheit, Datenschutz und einfache Bedienbarkeit“ legt. Die Postfächer sind frei von Werbung, es gibt kein Tracking, keine IP-Speicherung und auch keine Weitergabe persönlicher Daten (<https://posteo.de/site/datenschutz>). Zudem werden alle Mails mit verschiedenen Technologien verschlüsselt (<https://posteo.de/site/verschlueselung>). Die Posteo-Rechenzentren befinden sich in Berlin, Bielefeld und Frankfurt am Main, die Server werden mit „100 Prozent Ökostrom“ von Greenpeace Energy betrieben (<https://posteo.de/site/nachhaltigkeit>). Posteo bietet diese und weitere Leistungen allerdings nicht umsonst an: Nutzer müssen für ein Standard-Postfach mit zwei Gigabyte Speicherplatz, zwei Alias-Adressen und einem Online-Kalender einen Euro pro Monat bezahlen, kostenpflichtige Upgrades wie eine Speicherplatz-Erweiterung sind gegen Aufpreis möglich.



Posteo erklärt auf seiner Website, wie die Verschlüsselung der Mails erfolgt

Posteo

Posteo wurde 2009 gegründet. Die Zielsetzung der Gründer war es, eine E-Mail-Alternative für all jene Menschen zu bieten, die Wert auf Sicherheit, Datenschutz und Nachhaltigkeit legen. Die NSA-Skandale gaben dem Startup Aufwind: Zahlreiche Medien berichteten über Posteo und empfahlen den E-Mail-Dienst als Alternative zu Gmail, GMX und Co., auch die Bundesdatenschutzbeauftragte Andrea Voßhoff lobte den deutschen Mail-Provider in einem Bericht (https://posteo.de/bfdi_pruefbericht.pdf). Das Unternehmen verzeichnet eigenen Angaben zufolge (https://posteo.de/site/ueber_posteo) ein jährliches Wachstum von über 100 Prozent, betreut aktuell über 200.000 Postfächer und besitzt keinerlei Schulden.

Jetzt WIRED Member werden und mit uns in die Zukunft starten!

Mit im Paket: 4 Magazin-Ausgaben im Jahr und der Member-Zugang zu exklusiven Inhalten auf

Mittlerweile fahnden Europa- und die Behörden verschiedener Länder gegen den oder die Hintermänner der aktuellen Ransomware-Angriffe. Bedeutet das nun, dass Posteo die Daten des Postfachinhabers herausrücken muss? „Ermittlungsbehörden können Inhaltsdaten beschlagnahmen, wenn ein richtiger Beschluss zur Beschaffung vorliegt“, sagte Posteo-Pressesprecherin Sabrina Loecherer (https://twitter.com/sabrinaloehr?lang=de) in dieser Woche. „Wir werden aber überhaupt keine Auskünfte an Ermittlungsbehörden oder Anbieter, wie die Bundespolizei, weitergeben.“

„Ermittlungen nicht zu gefährden.“



COLLECTIONS

Business (/Collection/business) jetzt sollte allen Unternehmen

Tech (/Collection/tech) klar sein: Sie müssen ihre Firmenrechner

unbedingt gegen die aktuellen Angriffe schützen,

indem die IT-Abteilung das dringend nötige

Sicherheitsupdate für Windows

Gadgets (/Collection/gadgets)

(https://technet.microsoft.com/de-de/library

life/Collection/171040.aspx) herunterlädt und auf

allen Computern installiert.

Science (/Collection/science)

Design (/Collection/design)

HACKER (/COLLECTION/TAG/HACKER)

STARTUP (/COLLECTION/TAG/STARTUP)

SUBSCRIPTION

Membership (/Membership.wired.de)

Newsletter (Http://newsletter.wired.de) (//www.facebook.com/wired.de?subject=Wie%20die%20Ransomware-

FOLLOW US

SECTIONS

Video (/Video)

Magazin (/Magazin)

Collections (/Collection)

Conference

(Https://conference.wired.de)

Campus (Https://campus.wired.de)

Newsletter (Http://newsletter.wired.de)

OUR BRANDS

GQ (Http://www.gq-magazin.de/)

Glamour (Http://www.glamour.de/)

Vogue (Http://www.vogue.de)

Facebook (<https://www.facebook.com/WIREDGermany>)

AD (<http://www.ad-magazin.de>)

Twitter (https://twitter.com/WIRED_Germany)

Instagram (<https://www.instagram.com/wiredgermany/>)

Youtube (<https://www.youtube.com/user/WIREDde>)

Xing (<https://www.xing.com/news/pages/wired-germany-79>)

[IMPRESSUM \(/SERVICE/IMPRESSUM\)](#) [DATENSCHUTZ \(/SERVICE/DATENSCHUTZ\)](#) [AGB \(/SERVICE/AGB\)](#)
[NUTZUNGSBEDINGUNGEN \(/SERVICE/NUTZUNGSBEDINGUNGEN\)](#)
[JOBS \(HTTP://WWW.CONDENAST.DE/DE/JOBS-UND-KARRIERE\)](http://www.condenast.de/de/jobs-und-karriere) [WERBUNG \(/SERVICE/WERBUNG\)](#)
[MEMBERSHIP \(HTTP://MEMBERSHIP.WIRED.DE/?PROMO=HOMEPAGE_FOOTER_LINK\)](http://membership.wired.de/?promo=homepage_footer_link)
[RSS \(HTTPS://WWW.WIRED.DE/FEED/LATEST\)](https://www.wired.de/feed/latest) [WIRED CAMPUS \(HTTPS://WWW.WIRED.DE/CAMPUS\)](https://www.wired.de/campus)
[NEWSLETTER \(HTTP://NEWSLETTER.WIRED.DE/\)](http://newsletter.wired.de/)

 (http://www.condenast.de)