

28. Januar 2020, 15:35 Uhr IT-Gutachten

Hacker-Angriff auf Berliner Gericht massiver als bislang bekannt



Auf den Servern des Berliner Kammergerichts lagern sensible Daten. Wenn sie angegriffen werden, ist das höchstproblematisch. (Foto: Mike Wolff/imagio)

- Ein Hacker-Angriff auf das Berliner Kammergericht mit dem Trojaner "Emotet" ist weitaus gravierender gewesen als bislang bekannt.
- Einer Untersuchung zufolge war der Angreifer "höchstwahrscheinlich" in der Lage, den "gesamten Datenbestand des Kammergerichts zu exfiltrieren und zu manipulieren".
- Offen ist, warum das entsprechende Gutachten erst an diesem Montag publik geworden ist. Fachpolitiker mehrerer Parteien hatten schon seit Längerem auf Einblick in die Untersuchungen gedrängt.

Von Jan Heidtmann, Max Hoppenstedt und Simon Hurtz, Berlin



Facebook



Twitter



WhatsApp



E-Mail



Flipboard



Pocket



Drucken

Bislang war es nur einer von diesen Hacker-Angriffen, wie sie inzwischen immer wieder vorkommen: Schadsoftware wird gefunden, Rechner müssen vom Netz genommen werden. In der vergangenen Woche erging es ganz Potsdam so und auch der Stadt Brandenburg. Ende September hatte es das Berliner Kammergericht erwischt, dessen digitale Außenkommunikation daraufhin über Wochen lahmgelegt war.

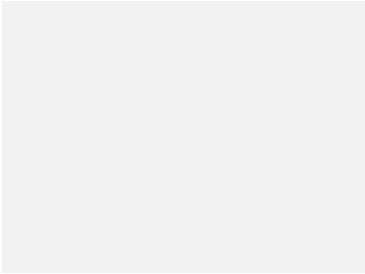
Nun zeigt sich, dass der Angriff offenbar weitaus massiver war als bisher angenommen.

Am vergangenen Freitag wurde das Ergebnis einer Untersuchung durch IT-Experten intern vorgestellt. "Vorläufiger forensischer Abschlussbericht zur Untersuchung des Incidents beim Berliner Kammergericht" nennt der IT-Dienstleister T-Systems das Gutachten, über das der *Berliner Tagesspiegel* [zuerst berichtete](#). Der entscheidende Satz lautet: "Wir weisen jedoch ausdrücklich darauf hin, dass ein Angreifer höchstwahrscheinlich in der Lage gewesen ist, (...) den gesamten Datenbestand des Kammergerichts zu exfiltrieren und zu manipulieren."

Das Berliner Kammergericht ist Berlins höchste Instanz für Straf- und Zivilsachen, vergleichbar mit einem Oberlandesgericht in anderen Bundesländern. Immer wieder werden Terror- oder Staatsschutzverfahren verhandelt, auf den Servern des Gerichts könnten auch Namen und Informationen zu verdeckten Ermittlern, Informanten und zahlreichen Zeugen in sensiblen Prozessen zu finden sein.

Warnung vor "Emotet"

"Gefährlichste Schadsoftware der Welt" befällt Bundesbehörden



Achtung, wenn vom Staat eine E-Mail kommt! Es könnten Kriminelle dahinterstecken. Deutschlands oberste Cyberwächter warnen vor schwer zu enttarnendem Spam.

Ende September war in den IT-Systemen des Kammergerichts der Trojaner "Emotet" festgestellt worden. Das Programm treibt seit dem vergangenen Jahr in Deutschland sein Unwesen, ursprünglich war es angelegt, um Zugangsdaten zum Online-Banking auszuspähen. Es verbreitet sich meist über fingierte E-Mail-Anhänge und ist so mutmaßlich auch in das System des Kammergerichts gelangt. Die Gutachter von T-Systems konnten feststellen, dass der Trojaner besonders darauf ausgelegt war, Passwörter von den Gerichtsrechnern zu klauen.

Dass Kennungen von Beamten aber tatsächlich für schädliche Zwecke missbraucht wurden, hält der Gerichtssprecher für eher unwahrscheinlich. "Die Passwörter nutzen ja jetzt nichts mehr, weil wir das Kammergericht vom Netz getrennt haben", sagt Thomas Heymann. Da der genaue Zeitpunkt des Angriffs auch von den Gutachtern nicht

ermittelt werden konnte, kann dies bis zum Abschalten der Rechner dennoch geschehen sein.

Die Berliner Datenschutzbeauftragte Maja Smolczyk teilte mit, dass aufgrund des Gutachtens keine definitive Aussage dazu gemacht werden könne, ob Daten "ausgeleitet" worden seien. "Es ist jedoch sehr wahrscheinlich, dass zumindest einige Zugangs- und andere Daten abgeflossen sind." Da es sich bei den am Kammergericht verarbeiteten Daten um "höchst sensitive Informationen" handle, habe man es "mit einem besonders schwerwiegenden Eingriff in die Rechte und Freiheiten der betroffenen Personen" zu tun. Dessen Folgen seien nur schwer einzugrenzen.

"Wenn es dazu gekommen sein sollte, dass Daten tatsächlich abgeflossen sind, wäre das der Super-Gau", sagt Sven Rissmann, rechtspolitischer Sprecher der CDU-Fraktion im Berliner Abgeordnetenhaus. "Unvorstellbar, wenn diese Prozessdaten in falsche oder kriminelle Hände gelangen", sagt Sven Kohlmeier, netzpolitischer Sprecher der SPD-Fraktion. "Da wird die Justizverwaltung noch viele Fragen beantworten müssen, um das Vertrauen in den Rechtsstaat an dieser Stelle wiederherzustellen."

Sowohl Berlins Justizsenator Dirk Behrendt von den Grünen als auch Gerichtspräsident Bernd Pickel hatten den möglichen Schaden des Hacker-Angriffs bislang eher heruntergespielt. So sagte Behrendt in einer Anhörung des Rechtsausschusses des Berliner Abgeordnetenhaus im Oktober, "dass wir momentan nicht davon ausgehen, dass es sich um einen gezielten Angriff auf die IT-Infrastruktur des Kammergerichts handelte." Ähnlich äußerte sich auch Gerichtspräsident Pickel.

IT-Experten raten zu "komplettem Neuaufbau" der IT-Infrastruktur des Gerichts

Offen ist, weshalb die Abgeordneten und auch die Öffentlichkeit erst jetzt informiert werden. Eine erste Fassung des Gutachtens kursierte schon kurz vor Weihnachten, der Verwaltung wurde die endgültige Fassung am 24. Januar vorgestellt. Fachpolitiker mehrerer Parteien hatten jedoch schon wochenlang gefordert, Pickel solle die Erkenntnisse veröffentlichen oder ihnen wenigstens Einsicht gewähren.

Präsident Pickel argumentiert, in dem Gutachten seien Aufbau und Wirkungsweise des Virus beschrieben - Informationen, die nicht öffentlich werden dürften, um weitere Angriffe zu verhindern. Nach

Angaben eines Sprechers des Justizsenats soll selbst Justizsenator Dirk Behrendt erst am Freitag über die Dimension des Angriffs informiert worden sein. Das wäre ein erstaunlicher Vorgang, da ein Hackerangriff diesen Ausmaßes auch für anderen Gerichte relevant sein könnte.

In ihrem Gutachten lassen die IT-Experten keinen Zweifel daran, wie wenig die bisherigen Sicherheitsvorkehrungen des Kammergerichts taugen: "Die IT-Infrastruktur des Kammergerichts ist nicht ausreichend vor Angriffen geschützt." Es könne nicht ausgeschlossen werden, dass die gesamte IT-Infrastruktur kompromittiert wurde. Deshalb raten die Experten zu einem "kompletten Neuaufbau".

So könnte das Debakel immerhin ein Gutes haben: Das Kammergericht könne die Situation nutzen, "um ein leistungsfähiges und sicheres neues Netzwerk zu konstruieren und den Schaden bei zukünftigen Vorfällen stark zu begrenzen", schreiben die Gutachter.

© SZ.de/gal [Feedback](#)



Facebook



Twitter



WhatsApp



E-Mail



Flipboard



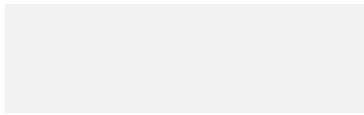
Pocket



Drucken

Cyberangriffe

Brandenburg fährt die Server runter



In Potsdam und der Stadt Brandenburg funktioniert die IT der Verwaltung nicht mehr, und eine Gemeinde geht prophylaktisch vom Netz. Vor der Schwachstelle hatten Fachleute schon zu Weihnachten gewarnt.

Von Jan Heidtmann, Berlin, und Valentin Dornis

Lesen Sie mehr zum Thema

IT-Sicherheit

Cyber-Angriff

Trojaner

Zur SZ-Startseite

Mehr zum Thema: IT-Sicherheit

Schadsoftware

USA

Covid-19

Covid-19-Impfstoff

Hack gegen Twitter

**Fitnesstracker-
Hersteller Garmin
bestätigt Cyberangriff**

**Chinesische Hacker
sollen
Geschäftsgeheimnisse
gestohlen haben**

**Impfstoff-Forschung
als Spielstein der
Mächte**

**Großbritannien
bezieht Russland,
Corona-Forscher zu
hacken**

Angriff im Gott-Modus

IT-Sicherheit
**Das waren die
spektakulärsten
Hackerangriffe**

Zehn Jahre Stuxnet
**Der Hack, der die Welt
aufschreckte**

Verschlüsselte Chats
**Polizei hackt sich in
schmutzige
Geheimnisse von
Killern und Dealern**

Datenleck
**Daten von 200 000
deutschen Foodora-
Nutzern geleakt**

Spionage-Software
**China soll jahrelang
Handys von Uiguren
überwacht haben**

VERLAGSANGEBOTE

SZ Stellenmarkt

Junior Systemingenieur* Fahrwerkregelsysteme Automotive

EDAG Engineering GmbH
80331 München

Bilanzbuchhalter/Finanzbuchhalter (m/w/d)

TOPOS Personalberatung Hamburg
20095 Hamburg

Facharzt für Orthopädie / Unfallchirurgie (m/w/d)

ZAR Nanz medico Zentrum für ambulante
Rehabilitation
66849 Landstuhl (Sickingenstadt), 6684...

Leser empfehlen im Ressort Digital

- 1** US-Wahlkampf **Trump: "Ich bin kognitiv da"**
- 2** Corona und Gastronomie **"Es gibt keinen besseren Zeitpunkt, um die Kneipen aufzumachen, als jetzt"**
- 3** American Football **Es ist perfide, was Washington da veranstaltet**

Meistgelesene Artikel

- 1** Nachruf **Verschmitzt, frech, leidenschaftlich**
- 2** Trumps Wahlverlegungsidee **Ein beispielloser Vorgang**
- 3** Trauerfeier für John Lewis **Verneigung ohne Trump**

ANZEIGE

GUTSCHEINE

GUTSCHEIN	%	GUTSCHEIN	%	GUTSCHEIN	%	GUTSCHEIN	%	GUTSCHEIN
50%		20%		10%		20%		Gr
50% OTTO Gutscheincode		20% Baurutschein		10% eBay Gutscheincode		20% Amazon Gutscheincode		Gra Gut

[Elektronik-Gutscheine](#) [Alle Shops](#)

ANZEIGE

VERGLEICHSPORTAL

[Produktvergleiche](#) → [Computerprodukte](#) → [Beamer Test](#) → [Externe Festplatte Test](#) → [Kop](#)

[Elektronikprodukte](#) → [Bluetooth Lautsprech...](#) → [Drucker Test](#) → [Fernseher Vergleich](#) → [Sma](#)

[Handytarife](#) [Handyvertrag](#)

[Zur SZ-Startseite](#)

[Datenschutz](#) [Nutzungsbasierte Onlinewerbung](#) [Mediadaten](#) [Newsletter](#) [Eilmeldungen](#) [RSS](#) [Apps](#) [AGB](#) [Jobs bei der SZ Digitale Medien](#)
[Kontakt und Impressum](#)

Copyright © Süddeutsche Zeitung Digitale Medien GmbH / Süddeutsche Zeitung GmbH