
Spur nach China?

# Bayer AG von Hackern ausgespäht

Stand: 04.04.2019 06:00 Uhr

**Der Dax-Konzern Bayer ist von der mutmaßlich chinesischen "Winnti"-Gruppe digital ausgespäht worden. Nach Informationen von *BR* und *NDR* war die Schadsoftware bis Ende März im Netzwerk des Konzerns zu finden.**

Von Hakan Tanriverdi, Maximilian Richt (BR) und Svea Eckert, Reiko Pinkert (NDR)

Hackerangriff auf den Bayer-Konzern: Die Hackergruppe "Winnti" soll im Auftrag des chinesischen Staates agieren. Davon gehen sowohl IT-Sicherheitsexperten als auch deutsche Sicherheitsbehörden aus. Es wird vermutet, dass dieselbe Gruppe 2016 auch den Dax-Konzern ThyssenKrupp infiltriert hatte.

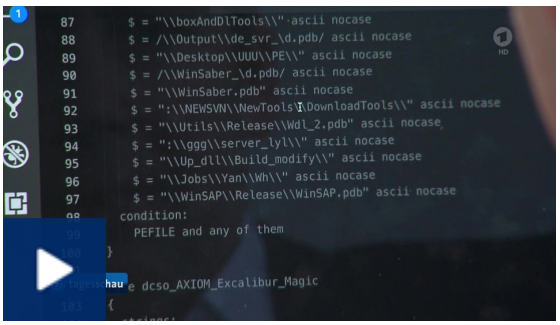
Bayer bestätigt auf Anfrage, dass die Hacker in das Netzwerk des Konzerns eindringen konnten: "Unser Cyber Defense Center hat Anfang 2018 Anzeichen von 'Winnti'-Infektionen detektiert und umfangreiche Analysen gestartet", teilt der Konzern schriftlich mit. Es lasse sich nicht rekonstruieren, seit wann die Hacker im Bayer-Netz aktiv waren.


Bayer bestätigt Anzeichen von "Winnti"-Infektionen.

## Zielgerichteter Angriff

"Wenn ein Unternehmen feststellt, dass es die 'Winnti'-Schadsoftware auf einem oder mehreren Rechnern hat, dann ist klar, dass es sich um einen zielgerichteten Angriff handelt", sagt Andreas Rohr, Leiter für Technik bei der Deutschen Cyber-Sicherheitsorganisation (DCSO). Diese wurde 2015 von verschiedenen Unternehmen, darunter Bayer, gegründet - und für die Aufklärung der Späh-Aktion hinzugezogen. Rohr sagt, Unternehmen müssten sich die Frage stellen, "wie groß die Kompromittierung, sprich der Befall im gesamten Netzwerk" sei. Die "Winnti"-Gruppe sei bekannt dafür, sich sehr stark auszubreiten.

Die Hacker der Winnti-Gruppe haben nach Angaben von Bayer insbesondere "Systeme an der Schnittstelle vom Intranet zum Internet sowie Autorisierungssysteme" infiziert. Die Hacker sollen hochprofessionell vorgegangen sein.




**Video: Hacker-Angriff auf Chemiekonzern Bayer**
tagesschau 16:00 Uhr, 04.04.2019, S. Eckert, H. Tanriverdi, M. Richt

Bayer gibt an, dass es keine "Evidenz für einen Datenverlust" gebe. Ein mit der "Winnti"-Schadsoftware infiziertes System hatten Datenjournalisten des *BR* mit Hilfe eines Netz-Scans gefunden und daraufhin den Konzern kontaktiert. Ende März seien die Systeme bereinigt worden, teilt Bayer mit: "Bis zu diesem Zeitpunkt sind die Angreifer nach unseren Erkenntnissen nicht aktiv geworden, um Informationen auszuleiten."

### Ermittlungen eingeleitet

Der Konzern stellte Strafanzeige. Die bei der Staatsanwaltschaft Köln angesiedelte Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW) bestätigt den Vorfall, will sich aber aus "ermittlungstaktischen Gründen" derzeit nicht äußern.

Neben der Spähaktion beim Dax-Konzern fand sich die "Winnti"-Schadsoftware nach Informationen von *BR* und *NDR* seit Anfang des Jahres bei mindestens drei Unternehmen aus dem deutschen Mittelstand. Das für IT-Sicherheit zuständige Bundesamt für Sicherheit in der Informationstechnik (BSI) teilt auf Nachfrage mit, dass es sich um Firmen handele, die im Bereich "Chemie, Maschinen- und Anlagenbau sowie Software" tätig sind. Das BSI warnt, die Bedrohungslage im Cyber-Raum sei für die deutsche Wirtschaft auf einem angespannt hohen Niveau.

Bereits 2016 gab es einen Vorfall, bei dem "Winnti"-Schadsoftware zum Einsatz kam: ThyssenKrupp. Florian Roth von der Firma Nextron Systems analysierte damals den Hacker-Angriff. "Bei 'Winnti' handelt es sich meiner Meinung nach um eines der am schwersten zu erkennenden Schadprogramme überhaupt", sagt Roth. Die Software hinterlasse kaum Spuren auf der Festplatte.

Chinas Ziel: Eine führende Wirtschaftsnation zu werden.

### Die Spur soll nach China führen

Der frühere BND-Präsident Gerhard Schindler, der heute als Berater arbeitet, weist darauf hin, dass die eindeutige Zuordnung einer Hackergruppe zu einem Land immer sehr schwierig sei. Cyber-Spionage bei deutschen Konzernen passe aber zu Chinas ehrgeizigen Wirtschaftszielen: China wolle "bis 2025 zu den führenden Wirtschaftsnationen aufschließen und bis 2049, also zum 100-jährigen Bestehen der Volksrepublik, zur mächtigsten Wirtschaftsnation der Welt werden", so Schindler.

Rohr von der DCSO erklärt ebenfalls, dass die von der Winnti-Gruppe ausgespähten Unternehmen in Chinas Pläne passen würden: "Von daher kann man davon ausgehen, dass da ein ganz gezielter Auftrag vom chinesischen Staat vorliegt." Zu 100 Prozent ließe sich das nicht beweisen.

### Verfassungsschutz warnt vor Wirtschaftsspionage

Auch der Bundestag beschäftigte sich immer wieder mit der Problematik. Zuletzt warnte ein Vertreter des Bundesamtes für Verfassungsschutz (BfV) im Januar dieses Jahres vor der chinesischen Wirtschaftsspionage. In einer vertraulichen Sitzung des Innenausschusses berichtete er, dass in Deutschland neben den großen, auch kleinere und auf Nischen spezialisierte Unternehmen im Fokus stünden. Diese könnten sich nämlich keine größeren IT-Sicherheitsteams leisten.

Bereits im September 2018 warnte das BfV die Abgeordneten vor dem neuen chinesischen Geheimdienstgesetz. Dieses räume den eigenen Behörden umfangreiche Sonderrechte ein, um nahezu ohne Einschränkungen im Ausland

nachrichtendienstlich tätig zu sein.

**Audio: Auch Bayer-Konzern Opfer von "Winnti-Hack"**
Svea Eckert, NDR, Hakan Tanriverdi, BR
03.04.2019 18:20 Uhr

**Über dieses Thema berichtete die tagesschau am 04. April 2019 um 12:00 Uhr.**

Bayer muss 80 Mio. Schadensersatz zahlen, 28.03.2019
Monsanto wird für Bayer zum Risiko, 28.03.2019
**Nachrichtenatlas** | Deutschland | Leverkusen