



## Deutsche Unternehmen im Fadenkreuz von Cyber-Angreifern - Einschätzung des ESET-IT-Sicherheitsexperten Thomas Uhlemann zum aktuellen Angriff auf die Bayer AG

"Deutsche Unternehmen leben von ihrer Innovationskraft und ihrem über Jahrzehnte aufgebautem branchenspezifischen Know-how. Nach Auskunft des Europäischen Patentamts haben allein 2017 deutsche Unternehmen mehr als 25.000 neue Patente angemeldet. Dieses wertvolle Wissen zu stehlen, ist seit Jahren für Online-Kriminelle und Cyber-Spione ein lukratives Geschäft. Der Schaden für die deutsche Wirtschaft ist immens und beziffert sich nach Einschätzung von Industrieverbänden und Ermittlungsbehörden auf mehr als 55 Milliarden Euro pro Jahr."

### Wie aufwendig sind derartige Angriffe auf Grossunternehmen? Und über welche finanziellen und technologischen Mittel müssen die Täter verfügen?

"Eine Attacke wie im aktuellen Fall ist für das jeweilige Ziel massgeschneidert. Eingesetzte Schadsoftware und andere Tools werden extra für diesen Angriff entwickelt und häufig nur für diesen Zweck benutzt. Das erschwert ein Auffinden durch automatisierte Systeme. Gleichzeitig bedeutet es, dass enorm viele Ressourcen aufseiten der Angreifer existieren müssen. Dazu zählen fähige Entwickler, entsprechende Infrastruktur und natürlich das Geld, um die Aktion zu finanzieren. Aber derartige Ausstattung verfügen in der Regel nur Milliarden-Konzerne oder eben Staaten. Die Mehrzahl der Angriffe, denen die deutsche Wirtschaft täglich ausgesetzt ist, ist jedoch "Massenware". Diese Malware hat nicht einzelne Firmen als Ziel, sondern versucht über massenhaft versandte Spammails in schlecht gesicherte IT-Systeme einzudringen. Berühmtestes Beispiel dafür sind aktuell sogenannte Ransomware- oder Verschlüsselungsstrojaner-Attacken."

### Wie lange bleiben erfolgreiche Angriffe auf Unternehmen verborgen?

"Es dauert durchschnittlich 180 Tage, bis Unternehmen bemerken, dass Angreifer sich an ihren Daten zu schaffen machen. In diesem halben Jahr können also Daten, Zugänge und andere sensible Informationen abgeschöpft werden. Oftmals fehlen jedoch entsprechende Verteidigungswerkzeuge, sodass die Dunkelziffer erfolgreicher Angriffe mit grosser Wahrscheinlichkeit weit höher ist. Sogenannte EDR (Endpoint Detection and Response) Tools können nachträglich helfen, Datenabflüsse zu entdecken und zurückzuverfolgen. Sie sind zwar am Markt verfügbar, werden aber selten genutzt."

### Wie hoch ist der durchschnittliche Schaden eines Cyber-Angriffs?

"Es hängt hierbei ganz von der Art des Angriffs und des entstandenen Schadens ab. Man kann sicherlich den finanziellen Schaden beziffern, der durch einen Produktionsausfall direkt entsteht. Die Folgekosten für die Wiederherstellung der Betriebsfähigkeit zählen genauso dazu, werden oft aber nicht mit angegeben. Reputations- und Vertrauensverlust aufseiten der Geschäftspartner und Kunden lässt sich dagegen oft schwer beziffern, ist aber unter Umständen geschäftsgefährdend. In die Schadensbetrachtung gehört zudem unbedingt eine mögliche Strafzahlung aufgrund der EU-DSGVO, wenn etwa Nutzer- oder Kundendaten gestohlen wurden, weil sie nicht ausreichend gesichert wurden. Sind geheime Produktionsunterlagen oder Pläne für kommende Produktgenerationen gestohlen worden, ist der Schaden nur schwer kalkulier- und versicherbar. Die Fälle der Vergangenheit, gerade bei grossen Firmen, haben jedoch einen Schaden im Millionenbereich entstehen lassen, wobei alle Folgen noch nicht abschätzbar sind. Die Hackerangriffe auf die Reederei Maersk hat einen geschätzten Schaden von bis zu 300 Millionen US-Dollar verursacht."

### Sind Dax-Konzerne besonders betroffen?

"Die Flaggschiffe der deutschen Wirtschaft stehen klar im Fokus der Cyber-Angreifer und Wirtschaftsspione. Unternehmen wie der Bayer-Konzern sind für potentielle Täter zweifellos lohnende Ziele. Das ergibt sich allein schon aus dem Wert der Daten, die potentielle Angreifer entwenden und für Millionen an zwielichtige Mitbewerber weiterverkaufen können. Erschwerend sind natürlich Angriffe, hinter denen einzelne Staaten vermutet werden. Cyberspionage scheint für einzelne Länder eine moderne Form der Wirtschaftsförderung zu sein. Im Vergleich zu mittelständischen Unternehmen verfügen Grosskonzerne über eigene Cyber-Abwehr-Zentren. Innovative Mittelständler können von derartigen Ressourcen natürlich nur träumen. Dabei verzeichnen wir gerade im KMU-Umfeld seit vielen Jahren eine deutliche Zunahme von Cyber-Angriffen. Diese sogenannten Hidden-Champions stehen klar auf der "Einkaufsliste" von Wirtschaftsspionen."

### Wer steckt hinter dem aktuellen Angriff auf den Bayer-Konzern? Ist es möglich zweifelsfrei einen Staat als Ursprungsland zu identifizieren?



"Verschiedene Experten ordnen die Attacke der Winnti Gruppe zu. Da es ein leichtes ist, seine Spuren zu verwischen oder falsche Fährten zu legen, ist eine eindeutige Zuordnung zu einem Staat oder einer verbrecherischen Grossorganisation nicht zweifelsfrei möglich. Die Winnti Gruppe ist jedoch für eine Reihe von Angriffen unterschiedlichster Natur verantwortlich. zu machen. Erst in März hat ESET einen Forschungsbericht veröffentlicht, in dem deutlich wird, dass Winnti vor allem asiatische Gamer und die Gaming-Industrie im Visier hatte.

### Wie können Unternehmen sich besser schützen - gerade, wenn sie nicht über die Ressourcen eines Grossunternehmens verfügen?

"Unternehmen, egal welcher Grösse, müssen verstehen, dass sie ein beliebtes Ziel für Kriminelle aller Art sind. Das Thema "IT-Security" kommt bei vielen Planungen noch zu kurz, wird schlecht budgetiert oder als Projekt betrachtet, dass mit dem Erwerb einer Antimalware-Lösung abgeschlossen werden kann. Die Sicherheit der zunehmenden Digitalisierung ist jedoch als permanenter Prozess zu verstehen, der innerhalb der Organisation auch gelebt werden muss. Die regelmässige Prüfung und Anpassung des Sicherheitskonzepts und auch die Schulung der eigenen Mitarbeiter ist hierbei zwingend erforderlich. Ein mehrschichtiger Verteidigungsansatz für alle Geräte und zusätzliche Tools, wie ESET Dynamic Threat Defense und ESET Enterprise Inspector können ein umfassendes Detection & Response-Konzept enorm unterstützen. Regelmässige Notfallübungen, inklusive der Überprüfung der Backup-Strategien für den digitalen Ernstfall, gehören ebenfalls zu einem guten Security-Prozess."