
# Schutzlos ausgeliefert?

## Massive Cyber-Angriffswelle auf Behörden, Onlineshops & Co.

**Cyberangriffe haben eine ganz neue Qualität erreicht, wie unter anderem der Hack von MediaMarkt und Saturn kurz vor dem wichtigen Weihnachtsgeschäft zeigt. Haben wir das Katz-und-Maus-Spiel gegen die Cyberbanden längst verloren? Nicht ganz, denn internationalen Fahndern sind jüngst hochkarätige Hintermänner ins Netz gegangen.**

**Von Ronald Eikenberg und Jürgen Schmidt**

Wer die aktuelle Nachrichtenlage verfolgt, dem werden vor allem zwei Themenbereiche immer wieder begegnen: Corona und Cyber-Erpressungen. Manchmal sogar beides in Kombination, wie im Fall des grauen Flecks auf der Corona-Landkarte des Robert-Koch-Instituts. Während allerorts die vierte Welle bereits mit voller Wucht zugeschlagen hatte, wirkte der Landkreis Ludwigslust-Parchim im Südwesten Mecklenburg-Vorpommerns mit null Neuinfektionen wie eine Insel der Glückseligen.

Der Landkreis konnte die durchaus existenten Infektionen aufgrund eines Hackerangriffs auf den kommunalen IT-Dienstleister KSM/SI nicht an das RKI melden. Betroffen war unter anderem die SORMAS-Schnittstelle, die beim Fallmanagement und zur Kontaktnachverfolgung in der Coronakrise zum Einsatz kommt.

Dieser ist nur einer von vielen aktuellen Fällen, in denen Cyber-Erpresser Chaos verursachen, wobei der graue Fleck auf der Landkarte nur ein Kollateralschaden war. Neben Behörden und Verwaltungen trifft es immer wieder auch Krankenhäuser sowie kleine und große Konzerne wie die Ceconomy AG, zu der die rund 1000 Märkte der Ketten MediaMarkt und Saturn gehören. Im anlaufenden Weihnachtsgeschäft hatten Cyber-Erpresser einen Kryptotrojaner von der Leine gelassen. Es traf Berichten zufolge über 3000 Server des Handelsriesen, der daraufhin seine Mitarbeiter aufgefordert haben soll, die Kassen vom Netz zu nehmen und Computer nicht zu benutzen.

### Kritische Infrastruktur

Den Betroffenen bleibt in solchen Fällen meist erst mal nichts anderes übrig, als die Stecker zu ziehen. Die mittelständische Kisters AG aus Aachen war nach einem Cyberangriff in der Nacht vom 10. auf den 11. November nicht mal mehr telefonisch über ihre Festnetznummer erreichbar. Dieser Fall ist besonders brisant, da das Unternehmen im Bereich der kritischen Infrastruktur tätig ist, es versorgt die Energiewirtschaft mit Software – Energieerzeuger, Netzbetreiber, Messstellenbetreiber und so weiter müssen sich also darauf verlassen können, dass die Kisters-Programme ordnungsgemäß arbeiten.

Das Unternehmen erklärte, es gebe „nach den bisherigen forensischen Analysen [...] keine Anzeichen dafür, dass die ausgelieferten Softwareprodukte kompromittiert sind“. Glück im Unglück.

### Bekannt, aber bewährt

In aller Regel steigen die Cybergangs über das schwächste Glied in der Kette in die Infrastruktur ein und breiten sich dann im Netz aus (siehe c’t 22/2021, S. 136). Das sind vor allem unvorbereitete Mitarbeiter, die durch gut gemachte Phishing-Mails aufs Glatteis geführt werden. Aber auch Fernzugänge via RDP oder VPN, die nicht durch Zwei-Faktor-Authentifizierung geschützt werden, haben die Angreifer im Visier. Und schließlich sind Dienste mit bekannten, aber noch nicht gepatchten Sicherheitslücken ein beliebtes Einfallstor.

Dem initialen Einbruch ins Netz folgt eine Phase, in der das Opfer ausgekundschaftet wird und die Angreifer sich weiter im Netz vorarbeiten. Dann kopieren und verschlüsseln die Eindringlinge alles, was ihren Opfern lieb und insbesondere teuer ist, ehe sie ein möglichst hohes Lösegeld in einer Kryptowährung fordern.

Die Liste der Hacks ließe sich beliebig fortführen. Viele Vorfälle schlagen keine großen Wellen, etwa weil es das Unternehmen schafft, so lange wie möglich den Mantel des Schweigens darüberzulegen. Das geht dann so lange gut, bis die Erpresser die abgesaugten Daten ins Darknet stellen, um den Druck zu erhöhen.

## Handel mit Zugängen

Die Cybercrime-Gangs entwickeln sich kontinuierlich weiter, sind untereinander gut vernetzt und spezialisieren sich immer weiter. Daraus entsteht dann ein Geflecht von kriminellen Banden, die sich gegenseitig ergänzen. Gerade hat sich ein neues Geschäftsfeld etabliert: Sogenannte Initial Access Broker (IAB) verkaufen Zugänge zu Firmennetzen. Das war früher eine Spezialität der berüchtigten Emotet-Bande. Doch nachdem im Januar Europol deren Infrastruktur komplett zerschlagen hatte, sprang eine Reihe von anderen Banden in die sich auftuende Marktlücke.

Mittlerweile gibt es einen florierenden Handel mit Zugängen zu lukrativen Opfern, teilweise halböffentlich über Untergrundforen beziehungsweise -Marktplätze, zum Teil aber auch direkt über persönliche Beziehungen. Bezahlt wird dabei je nach Qualität des Zugangs – Domain-Admin-Rechte, mit denen man die Hoheit übers Netzwerk gewinnt, bedeuten einen heftigen Preisaufschlag. Die eigentliche Erpressung, also das Stehlen von Daten und deren Verschlüsselung, übernehmen dann erst die Käufer.

Durch das Aufkommen von Ransomware-as-a-Service (RaaS) hat sich die Zahl der aktiven Gruppen vervielfacht und viele von denen haben selbst gar nicht die Expertise, einen erfolgreichen Einbruch durchzuführen. Diese Affiliates arbeiten dann lediglich vorgefertigte Listen ab, die etwa Schritt für Schritt beschreiben, wie man die Backup-Server findet oder Ransomware im Netz verbreitet. Sie kaufen beim IAB ihres Vertrauens Zugänge zu lukrativen Zielen und führen dann die eigentliche Erpressung durch. Das Waschen des Lösegelds übernimmt wieder der RaaS-Anbieter, der dann dem Affiliate seinen Anteil auszahlt.

Auch wenn sich der Eindruck aufdrängt, dass langfristig kein System den Machenschaften der professionellen Cybergangs standhalten kann, wäre es ein Trugschluss, die Flinte ins Korn zu werfen, weil ein erfolgreicher Angriff scheinbar unvermeidlich ist. Es mag sein, dass ein Angreifer mit unbegrenztem Budget früher oder später sämtliche Hürden überwinden kann. Dennoch muss der Anspruch stets sein, den Aufwand für den Angreifer so groß wie nur möglich zu gestalten.

## Druck erhöhen

Darüber hinaus muss es auch Druck auf die Kriminellen geben. Lange Zeit sah es so aus, als könnten sie Millionensummen abkassieren, ohne Konsequenzen befürchten zu müssen.

Die Ermittlungsbehörden sind allerdings keineswegs untätig, wie der wichtige Schlag gegen die berüchtigte Emotet-Gang zeigt. Einzelne Fahndungserfolge wie dieser bringen aber erst mal wenig – sie führen nur dazu, dass andere eine Chance sehen, die frei gewordene Position zu besetzen. Jedoch steigt der Druck auf die Cybercrime-Szene offenbar. Er hat bereits dazu geführt, dass sich zwei der großen RaaS-Banden zurückgezogen haben: DarkSide und REvil dominierten 2021 die Schlagzeilen unter anderem mit ihren Angriffen auf den wichtigen Pipeline-Betreiber Colonial und die Admin-Software Kaseya VSA. Insbesondere die Kaseya-Angriffswelle von REvil hatte weitreichende Konsequenzen. Bis zu 1500 Unternehmen wurden erpresst.

Doch mit dem Rückzug konnten sich die Täter nicht der Strafverfolgung entziehen: Wie Europol meldete, gelang es einem internationalen Ermittlerverbund gerade, zwei Verdächtige zu verhaften, die aus dem REvil-Umfeld stammen und für 5000 Infektionen verantwortlich sein sollen. Der Erfolg geht auf das Konto der Operation GoldDust, an der Ermittler aus 17 Ländern beteiligt waren sowie Europol, Eurojust und Interpol. Das lässt ahnen, wie aufwendig es ist, der Cybergangs habhaft zu werden.

Anfang Oktober konnte an der polnischen Grenze zudem ein Ukrainer aufgegriffen werden, nach dem die USA per internationalem Haftbefehl gesucht hatten. Er soll an der Kaseya-Angriffswelle beteiligt gewesen sein. Die Erfolge gegen solche hochrangigen Ransomware-as-a-Service-Anbieter sind sehr wertvoll, da diese Gangs Infrastruktur und Know-how bereitstellen. Letztlich gibt es da nur ein paar Handvoll aktiver RaaS-Banden auf hohem Niveau. Nach REvil und DarkSide wäre die Bande hinter der Conti-Ransomware der nächste große Akteur.

Insgesamt berichtet Europol von bislang sieben Verhaftungen im Kontext mit REvil und der mutmaßlichen Vorgängerbande GandCrab. Das US-Außenministerium hat unterdessen ein Kopfgeld von 10 Millionen US-Dollar für Hinweise ausgesetzt, die zur Identifizierung weiterer Schlüsselfiguren im Fall REvil führen – seit jeher ein bewährtes Mittel, um Schurken ins Kittchen zu bringen.

## Fazit

Der Kampf gegen Cybercrime ist nicht so aussichtslos, wie er lange Zeit schien. Das organisierte Verbrechen hat keine magischen Superkräfte und ist auch nicht unangreifbar. Wichtig ist jetzt, dass die internationale Gemeinschaft den Druck auf Cybercrime-Akteure weiter erhöht. Aber das bedeutet nicht, dass Firmen und Verwaltung in ihrer Wachsamkeit nachlassen dürfen. Nur wenn die Anstrengungen auf beiden Ebenen weitergehen – sich also Firmen besser schützen und Erpresser reale Konsequenzen fürchten müssen – kann es gelingen, den Siegeszug der Cybercrime zu beenden. *(rei@ct.de)* c't

### heise Security Pro

Teile dieser Analyse stammen aus dem wöchentlichen Newsletter für heise Security Pro, in dem Senior Security Fellow Jürgen Schmidt regelmäßig über Hintergründe zum Thema Cybercrime berichtet:
https://heise.de/heisec-projetzt


**Kopfgeld gegen Lösegeld: Die US-Regierung hat 10 Millionen US-Dollar ausgeschrieben für Hinweise, die zur Identifizierung von Schlüsselfiguren der REvil-Bande führen.**