**Information Security World 2022**

**Mit Ransomware leben und die Gefahren minimieren**

**München | Bad Homburg, Deutschland – 7. Juni 2022** – Ein 100-prozentiger Schutz vor Ransomware ist eine Illusion, zugleich kann aber eine Kapitulation auch nicht der Weisheit letzter Schluss sein. [NTT DATA DACH](https://de.nttdata.com/) und [NTT Ltd.](http://services.global.ntt/) (NTT Group) zeigen, welche Maßnahmen ein Unternehmen zur Gefahrenabwehr und Minimierung der Schäden ergreifen kann: von den Angriffsvektoren über die Angriffserkennung und schnelle Reaktion bis hin zur Optimierung der Infrastruktur nach einer erfolgten Attacke.

Dass Ransomware zu den größten Cyber-Gefahren zählt, ist unbestritten. Und Unternehmen können sich dem Risiko nicht entziehen, es gehört zum Alltag der IT. Auch eine Entschärfung der Bedrohungslage ist nicht in Sicht. Im Gegenteil: Schließlich tauchen permanent neue professionelle Tools oder Ransomware-as-a-Service-Angebote auf. Die Folgen eines Angriffs können gravierend sein: Die durchschnittlichen Ausfallzeiten von Unternehmen liegen bei rund drei Wochen. Und auch ein Angriff auf ganze Staaten ist nicht ausgeschlossen, wie [das aktuelle Beispiel Costa Rica](https://apnews.com/article/technology-government-and-politics-caribbean-gangs-381efc2320abb5356dee7f356e55e608) zeigt. Da Ransomware nicht verschwinden wird, sollte ein Umdenken erfolgen: Unternehmen müssen Security-Strategien und -Lösungen nutzen, die nicht nur auf die Vermeidung von Ransomware-Angriffen abzielen, sondern auch die Reaktion auf erfolgreiche Attacken adressieren. Nur so kann die Business Continuity gewährleistet werden.

Welche Maßnahmen helfen nun, die Gefahren in den Griff zu bekommen? Es sind vier Bereiche, in denen Unternehmen tätig werden sollten, um gegen Angriffe maximal gewappnet zu sein und mögliche Schäden auf ein Minimum zu begrenzen:

**1. Minimierung der Angriffsfläche**

Im Hinblick auf die unterschiedlichen Angriffsvektoren, die von Phishing über Brute-Force- bis hin zu Supply-Chain-Attacken reichen, können Unternehmen verschiedene Sicherheitsmaßnahmen ergreifen. Dazu zählen etwa die Implementierung einer IAM (Identity and Access Management)-Lösung für die Verwaltung von Identitäten, eine Mehr-Faktor-Authentifizierung oder die regelmäßige Installation von Updates und Patches, um Sicherheitslücken zu schließen. Neben kontinuierlichen allgemeinen Risikoanalysen bieten sich zudem gezielte Penetrations- und Vulnerability-Tests an. Auch eine Netzwerksegmentierung ist sinnvoll, um die Angriffsfläche möglichst gering zu halten. Dabei kann durchaus eine Mikro-Segmentierung in Betracht gezogen werden, die so weit gehen kann, dass jeder Rechner ein eigenes Netz darstellt. Auf diese Weise ist ein potenzieller Ransomware-Schaden auf ein Minimum begrenzt. Nicht zuletzt ist auch die Sensibilisierung der Mitarbeiter ein Teil einer umfassenden Sicherheitsstrategie: mit Schulungen zu potenziellen Bedrohungen und zu einem verantwortungsbewussten Umgang mit Systemen und Daten.

**2. Frühzeitige Angriffserkennung**

Von essenzieller Bedeutung ist die schnelle Erkennung eines Sicherheitsvorfalls. In vielen Fällen bleiben Ransomware-Angreifer zunächst unerkannt im Unternehmensnetz verborgen – teilweise bis zu 200 Tage –, bevor sie aktiv in Erscheinung treten. Das Problem dabei ist, dass dann das Unternehmensnetz weitgehend infiltriert sein kann und auch regelmäßige Backups von den Angreifern eventuell bereits verschlüsselt sind. So sind eine schnelle Wiederherstellung und Aufnahme des Regelbetriebs quasi unmöglich. Eine klassische Maßnahme für die Angriffserkennung ist die Analyse von Log-Files. Hilfreich sind dabei SIEM (Security Information and Event Management)-Systeme, die einen ganzheitlichen Blick

auf die IT-Sicherheit bieten, indem Log-Files und Meldungen verschiedener Lösungen gesammelt und ausgewertet werden. In Echtzeit kann ein Unternehmen damit verdächtige Ereignisse oder gefährliche Trends erkennen. Wer noch einen Schritt weiter gehen will, nutzt auch eine Deception-Lösung. Vereinfacht ausgedrückt leitet sie potenzielle Angreifer in die Irre und in eine überwachte Umgebung. So können Unternehmen Angriffe bereits im Anfangsstadium identifizieren und proaktiv unterbinden.

**3. Schnelle Reaktion**

Jedes Unternehmen sollte eine Incident-Response-Strategie etablieren, die konkrete Maßnahmen bei Sicherheitsvorfällen umfasst. Dazu gehören zum Beispiel die Festlegung von Verantwortlichkeiten, die Definition von Aufgaben, die Klassifizierung von Schadensfällen oder erforderliche Kommunikationsprozesse im Hinblick auf Strafverfolgungsbehörden – auch unter Beachtung etwaiger Meldepflichten. Konkret nutzt ein Unternehmen dabei dedizierte Ablauf- und Notfallpläne in Form von Playbooks, die eine schnelle und automatische Reaktion auf Vorfälle unterstützen. Eine adäquate Antwort erfordert immer auch eine unmittelbare Analyse des Sicherheitsvorfalles, also etwa hinsichtlich der aktuell beziehungsweise möglicherweise betroffenen Zielsysteme. Auf dieser Basis kann ein Unternehmen zielgerichtete Abwehrmaßnahmen ergreifen, zum Beispiel einzelne Systeme abschalten, bestimmte Netzwerkbereiche abtrennen oder alle Internetverbindungen vollständig deaktivieren. Anschließend geht es um die Wiederherstellung der Systeme und die Aufnahme des Normalbetriebs unter Nutzung der Backups. Um hierbei potenzielle Probleme auszuschließen, sollten Unternehmen regelmäßig ihre Backups und – was oft vergessen wird – auch die reibungslose und erfolgreiche Funktionsweise der Restore-Prozesse überprüfen.

**4. Optimierung der Infrastruktur**

Nach jedem Ransomware-Angriff muss auf jeden Fall die gesamte Infrastruktur auf den Prüfstand gestellt werden. Nur ausgehend von einer detaillierten forensischen Analyse des Angriffsszenarios können konkrete Abwehrmaßnahmen ergriffen werden, die eine Wiederholung verhindern. Dabei muss das exakte Angriffsmuster mit der zeitlichen Abfolge untersucht werden: vom ursprünglichen Angriffsvektor bis zur Verbreitung der Schadsoftware im Netzwerk. Die Überprüfung sollte dabei alle in der Vergangenheit betroffenen und in der Zukunft potenziell gefährdeten IT-Umgebungen berücksichtigen: von Betriebssystemen über Administrationskonsolen für Cloud-Services und Applikationen bis hin zu Konfigurations- und Anwenderdateien. Das heißt: Es geht in einem letzten Schritt zur Vermeidung künftiger Ransomware-Schäden um eine detaillierte Analyse mit anschließender Optimierung der Infrastruktur.

„Die Zahlen sprechen für sich: Ransomware und Phishing gehören weltweit zu den größten Bedrohungen für die IT-Sicherheit. Etliche Unternehmen schützen sich dabei immer noch unzureichend. Die Konsequenz kann ein Komplettausfall des Betriebs sein“, betont Bernhard Kretschmer, Vice President Service and Cybersecurity der NTT Ltd. in Deutschland. „Mit einigen zentralen Präventiv-Maßnahmen kann das Risiko eines solchen Supergaus deutlich reduziert werden. Die Minimierung der Angriffsfläche, die schnelle Erkennung von und Reaktion auf Ransomware sowie eine nachhaltige Optimierung der IT-Landschaft sind dabei die entscheidenden Faktoren.“

Patrick Schraut, Senior Vice President Cybersecurity DACH bei NTT DATA, ergänzt: „Mit Ransomware-Attacken werden Unternehmen auch in der Zukunft leben müssen. Will ein Unternehmen bei der Abwehr von Angriffen oder der Minimierung möglicher Schäden auf Nummer sicher gehen, kann es dabei auch auf die Dienste eines externen SOC – Security Operations Center – zurückgreifen. Es fungiert als proaktives Abwehrzentrum, in dem unter anderem die Früherkennung von Angriffen erfolgt – und zwar durch den Einsatz intelligenter Tools wie KI-gestützter Systeme, die eine permanente Analyse des Datenverkehrs und die Korrelation unterschiedlichster Informationen sicherstellen. Diese Aufgabe können Unternehmen alleine kaum leisten, deshalb gehen auch immer mehr den SOC-Weg in eine Ransomware-resistente Zukunft.“

**Über NTT DATA**

NTT DATA – ein Teil der NTT Group – ist Trusted Global Innovator von Business-, IT- und Telekommunikations-Lösungen mit Hauptsitz in Tokio. Wir unterstützen unsere Kunden bei ihrer Transformation durch Consulting, Branchenlösungen, Business Process Services, Digital- und IT-Modernisierung und Managed Services. Mit NTT DATA können Kunden und die Gesellschaft selbstbewusst in die digitale Zukunft gehen. Wir setzen uns für den langfristigen Erfolg unserer Kunden ein und kombinieren globale Präsenz mit lokaler Kundenbetreuung in über 50 Ländern. Weitere Informationen finden Sie unter [nttdata.com.](https://www.nttdata.com/global/en/)

**Pressekontakt für Deutschland, Österreich und Schweiz:**

|  |  |
| --- | --- |
| NTT DATA DACH  Cornelia Spitzer, BA  Press Manager DACH  Tel.: +43 664 8847 8903  E-Mail: [cornelia.spitzer@nttdata.com](mailto:cornelia.spitzer@nttdata.com) | Storymaker Agentur für Public Relations GmbH  Gabriela Ölschläger  Senior Consultant  Tel.: +49 7071 93872 217  E-Mail: [g.oelschlaeger@storymaker.de](mailto:g.oelschlaeger@storymaker.de) |

**Über NTT Ltd.**

NTT Ltd. ist ein führender, globaler Technologiedienstleister. Die weltweite Kompetenz, Expertise und umfassenden Technologiedienstleistungen, die über eine integrierte Serviceplattform bereitgestellt werden, helfen Kunden, die Digitale Transformation voranzutreiben. Als langfristiger, strategischer Partner unterstützt NTT Unternehmen bei der Verbesserung der Kunden- und Mitarbeitererfahrung, der Transformation der Cloud-Strategie, der Modernisierung von Netzwerken und der Stärkung der Cybersicherheit. Darüber hinaus automatisiert NTT die Geschäftsprozesse und IT von Unternehmen und zieht Erkenntnisse und Analysen aus deren Kerngeschäftsdaten. Als globaler ITK-Anbieter beschäftigt NTT mehr als 50.000 Mitarbeiter in 57 Ländern, betreibt Handel in 73 Ländern und bietet Dienstleistungen in über 200 Ländern und Regionen an. Together we enable the connected future.

Weitere Informationen unter [services.global.ntt](https://services.global.ntt/) und services.global.ntt/de-de/newsroom.

Bei Rückfragen wenden Sie sich bitte an:

|  |  |
| --- | --- |
| NTT Germany AG & Co. KG  Hakan Cakar  Vice President Marketing and Communications Germany  Tel.: +49 89 231217832  E-Mail: [hakan.cakar@global.ntt](file:///\\muc-nas-02.de.softlab.net\sl_muc\Marketing_Communications\_Intern\UNTERNEHMENSKOMMUNIKATION\Public%20Relations\Pressemitteilungen-News\NTT%20DATA\FY2021-2022\2021-06-29-PM-Launch-virtuelles-5G-Netzwerk-Enso\hakan.cakar@global.ntt) | **P**R-COM GmbH  Christina Haslbeck  Senior Account Manager  Tel.: +49 89-59997-702  E-Mail: [christina.haslbeck@pr-com.de](mailto:christina.haslbeck@pr-com.de) |