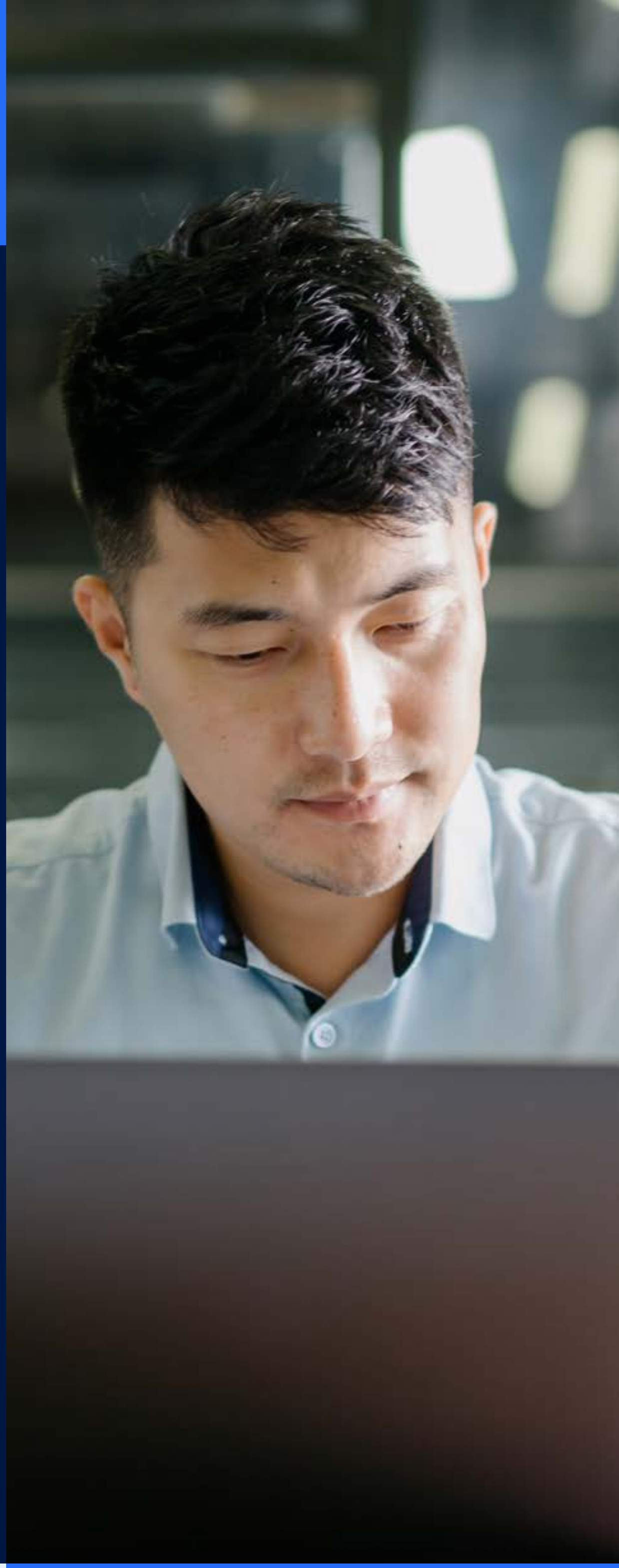
Die 40 häufigsten Ransomware-Techniken und wie man sie unterbindet

Leitfaden zur Umsetzung aktiver Abwehrmaßnahmen mit Deception-Technologie



WHITEPAPER

Inhaltsverzeichnis

Einführung

Mit der zunehmenden Anzahl von Vorfällen häufen sich auch die Ressourcen, die zum Thema Ransomware veröffentlicht werden. Die Verfasser solcher Whitepapers, Leitfäden und Reports arbeiten sich immer wieder am gleichen Schema ab: Einleitend werden besorgniserregende Fakten und Zahlen zum Ausmaß des Problems vorgestellt und neue Varianten erwähnt.
Im nächsten Absatz wird dann erst noch auf die am stärksten betroffenen Branchen eingegangen, bevor der Leser endlich ein paar halbwegs nützliche Tipps erhält.

Ransomware-Angriffe sind schlecht fürs Geschäft und jährlich fallen zahlreiche Unternehmen zum Opfer — das wissen Sie schon.

Wissen Sie aber auch, wie Sie solche Angriffe aktiv abwehren können?

Warum haben wir einen Leitfaden erstellt?

Sie tun bereits alles Mögliche, um Bedrohungen abzuwehren. Aber selbst die sichersten Unternehmen der Welt wissen: Absolute Sicherheit gibt es nicht. Es gibt jedoch einige einfache Maßnahmen, die weder teure Tools noch komplizierte Implementierungen erfordern und Ihre Ransomware-Abwehr spürbar verbessern.

Genau dabei soll dieser Leitfaden Sie unterstützen — mit konkreten Handlungsempfehlungen für Maßnahmen, die in Ihrer Kontrolle liegen und einen effektiven Schutz vor Ransomware-Angriffen gewährleisten. Alle vorgestellten Abwehrmaßnahmen zielen darauf ab, die Verbreitung von Ransomware einzudämmen und ihre Auswirkungen zu reduzieren.

Vorteile einer aktiven Abwehr mit Deception-Technologie zur Bekämpfung von Ransomware

Die meisten Sicherheitslösungen zielen auf isolierte Einzelaspekte ab:
Wollen Sie Endgeräte schützen? Nutzen Sie eine EDR-Lösung. Sie brauchen mehr Transparenz? NTA. Schädliche User-Aktivitäten? UEBA ist die Lösung.

Ransomware kann mit sämtlichen Bereichen Ihrer IT-Umgebung interagieren.
Abwehrmaßnahmen, die einzelne Teile schützen, sind daher nur sehr bedingt wirksam.
Zur erfolgreichen Abwehr von Ransomware ist stattdessen eine ganzheitliche Strategie erforderlich, die alle unternehmenskritischen IT-Ressourcen einbezieht.

Genau darum geht es bei der sogenannten aktiven Abwehr. Gemeint ist ein Ansatz, der sich an konkreten Anwendungsfällen orientiert und zu ausgewogenen Ergebnissen führt. Sie wählen den jeweils relevanten Anwendungsfall aus (hier also Schutz vor Ransomware) und setzen unternehmensspezifische Prioritäten für die Umsetzung (siehe dazu unsere Hinweise).

WIE LÄSST SICH RANSOMWARE MIT EINER AKTIVEN ABWEHRSTRATEGIE BEKÄMPFEN?

- Der Einsatz von Zscaler Deception zur Erstellung einer gefälschten Angriffsfläche bringt die Ransomware-Akteure aus dem Konzept und stört die Abläufe des Angriffs.
- Die reale Angriffsfläche der Organisation wird mithilfe hochgradig effektiver Kontrollmechanismen minimiert, sodass die Angreifer nur eingeschränkten Spielraum haben.
- Die verbleibende Angriffsfläche wird durch äußerst effektive Tricks überwacht, um die Angreifer bei der Ausführung ihrer verbleibenden Optionen in die Falle zu locken.

Hinweise zur Umsetzung

Wir empfehlen Ihnen, folgende Bereiche Ihrer IT-Umgebung zu priorisieren:

- DMZ
- Active Directory
- Unternehmenskritische Serversegmente
- User-Konten mit hoher Berechtigungsstufe
- Workstations mit hoher Berechtigungsstufe

Nachdem wirksame Maßnahmen zum Schutz dieser Kernbereiche eingerichtet wurden, kann eine breitere Umsetzung erwogen werden, sofern Ihre Organisation über entsprechende Ressourcen und Kapazitäten verfügt.

Einige der hier vorgestellten Techniken sind mit erheblichem Zeit- und Arbeitsaufwand verbunden. In diesem Zusammenhang weisen wir ausdrücklich darauf hin, dass die effektive Abwehr von Malware immer eine gewisse Einsatzbereitschaft erfordert. Um sicherzustellen, dass sich die in ihre Umsetzung investierte Mühe lohnt, werden in diesem Leitfaden nur solche Strategien berücksichtigt, deren Wirksamkeit in einem asymmetrischen Verhältnis zum jeweils erforderlichen Aufwand steht.

AN WEN RICHTET SICH DER LEITFADEN?

- Sicherheitsexperten, die auf einfache, bewährte Strategien gegen Ransomware setzen
- SOC-Analysten mit Führungsverantwortung
- SOC-Verantwortliche
- Alle, die sich für das Thema Ransomware und ihre Abwehr interessieren

Selbst wenn Sie nur einen Teil der Empfehlungen in diesem Leitfaden umsetzen, können Sie die Angriffsfläche, die Ihre Organisation Ransomware-Akteuren bietet, erheblich verkleinern. Damit ist schon viel gewonnen.

Auf geht's!

Wir wollen Ihnen die Umsetzung der vorgestellten Maßnahmen so einfach wie irgend möglich machen. Nachstehend wird eine Reihe von Ransomware-Techniken mit den jeweils dazugehörigen Abwehrmaßnahmen vorgestellt. Letztere sind darauf ausgelegt, die Technik entweder frühzeitig zu erkennen oder ihre Fähigkeit zur Ausbreitung einzuschränken. Ergänzt werden diese Informationen durch konkrete Hinweise zur Umsetzung der einzelnen Maßnahmen sowie Angaben zu ihrer Einordnung gemäß MITRE Engage Framework.

	RANSOMWARE-TAKTIK / -TECHNIK	GEGENMASSNAHME ZUR AKTIVEN ABWEHR	WIRKUNG	KNIFFE, TIPPS, TRICKS UND EMPFEHLUNGEN	EINORDNUNG GEMÄSS MITRE ENGAGE
1	ERSTINFIZIERUNG Infiziert öffentlich zugängliche IT-Ressourcen mit bekannten Sicherheitsrisiken (wie Wordpress/ CMS usw.)	Decoy-Anwendungen im Internet erstellen, die Ransomware-Angriffe auf öffentlich zugängliche Assets mit bekannten Schwachstellen abfangen	Erstellt eine gefälschte Angriffsfläche und behindert den Ablauf des Ransomware-Angriffs, indem den Akteuren ein vermeintliches Angriffsziel präsentiert wird	Decoys von CMS für Joomla oder Wordpress erstellen, die häufig von Angreifern ins Visier genommen werden	Vielfalt von Artefakten → Vielfalt von Anwendungen →
2	ERSTINFIZIERUNG Passwort-Spraying bei gängigen Anwendungen	Passwort-Spraying-Angriffe lassen sich mithilfe von Decoy-Anwendungen mit bekannten Standard-Passwörtern abfangen bzw. vereiteln	Erstellt eine gefälschte Angriffsfläche und behindert den Ablauf des Ransomware-Angriffs, indem den Akteuren ein vermeintliches Angriffsziel präsentiert wird	Decoys von Anwendungen wie Apache Tomcat und PhpMyAdmin erstellen	Vielfalt von Artefakten → Vielfalt von Anwendungen →
3	ERSTINFIZIERUNG Nutzt kürzlich bekannt gewordene Sicherheitslücken aus (z. B. die Schwachstelle in Microsoft Exchange)	Anwendungen mit kürzlich geschlossenen Sicherheitslücken sind bevorzugte Angriffsziele. Ransomware-Akteure können mithilfe von Decoys solcher Anwendungen dazu verleitet werden, ihre Anwesenheit preiszugeben.	Erstellt eine gefälschte Angriffsfläche und behindert den Ablauf des Ransomware-Angriffs, indem den Akteuren ein vermeintliches Angriffsziel präsentiert wird	Decoys für Anwendungen erstellen, bei denen kürzlich Sicherheitslücken offengelegt wurden (z. B. Microsoft Exchange und F5)	Vielfalt von Artefakten → Vielfalt von Anwendungen →
4	ERSTINFIZIERUNG Brute-Force-Angriff auf öffentlich zugängliche RDP-Server	• Eingehenden Zugriff auf den RDP-Port 3389 von der Host-/ Netzwerk-Firewall blockieren • Zugriff auf RDP nur für bekannte IP-Adressen zulassen (gilt insbesondere für Cloud-Server)	Durch Blockierung des Zugriffs auf RDP-Server wird die Angriffsfläche verkleinert, die für Ransomware-Akteure zugänglich ist, und damit die Ausbreitung der Ransomware eingedämmt	Der Zugriff auf RDP-Server kann über die Windows-Firewall oder Google Cloud Console blockiert werden.	Sicherheitskontrollen → Netzwerkmanipulation → Isolierung →
5	ERSTINFIZIERUNG Ausnutzung von Anwendungen, die mit Administratorrechten ausgeführt werden	DMZ-Anwendungen mit minimaler Rechtevergabe ausführen	DMZ-Anwendungen mit minimaler Rechtevergabe ausführen	Anwendungen mit minimaler Rechtevergabe ausführen	Administratorzugriff →

	RANSOMWARE-TAKTIK / -TECHNIK	AKTIVE ABWEHR	WIRKUNG	KNIFFE, TIPPS, TRICKS UND EMPFEHLUNGEN	EINORDNUNG GEMÄSS MITRE ENGAGE
6	ERSTINFIZIERUNG Ausnutzung von Anwendungen, die mit Administratorrechten ausgeführt werden	• PowerShell mithilfe von GPO/Anwendungssteuerung blockieren, wenn die Verwendung nicht erforderlich ist • Ausgehende Verbindungen über PowerShell mit Windows-Firewall überwachen • Protokollierung von PowerShell-Skriptblöcken aktivieren	• Verhindert die Ausführung von Commodity-Ransomware • Liefert Informationen über alle Internetverbindungen, die in einem kritischen Segment von PowerShell hergestellt wurden • Liefert Informationen darüber, welche PowerShell-Skripts ausgeführt wurden	Über GPO-Funktionen PowerShell blockieren, Überwachung aktivieren und Firewall-Zugriff steuern	Sicherheitskontrollen → Baseline ermitteln → Standardverfahren →
7	ERSTINFIZIERUNG Stellt vom infizierten DMZ-Segment aus eine Verbindung zu C2-Servern her	Whitelist für ausgehenden Internetzugang von der DMZ einrichten	Infektionen sind zwar möglich, das Fehlschlagen des C2-Rückrufs aus dem Segment stört jedoch den Angriffsablauf	Internetzugang durch Kombination aus Firewall für ausgehenden Traffic und Unternehmens-Proxy blockieren	Sicherheitskontrollen → Baseline ermitteln → Operatives Ziel →
8	ERSTINFIZIERUNG • Bettet sich in ein Makro ein • Verwendet DDE zum Ausführen von Code	• Makros über GPO entfernen • DDE über GPO deaktivieren • Geschützte Ansicht über GPO aktivieren GPO strategisch für User mit hoher Berechtigungsstufe bereitstellen (sowie User, die die Funktion nicht benötigen)	Verlangsamt Ransomware-Abläufe Verhindert gängige Techniken zum Einbetten von schädlichem Code, der für Erstinfizierungen verwendet wird	GPO-Vorlagen zur Steuerung von MS-Office-Funktionen verwenden E-Mail-Sicherheitsfunktionen können zum gleichen Zweck eingesetzt werden	E-Mail-Manipulation → Operatives Ziel →
9	PERSISTENZ Nistet sich über die Registry ein	„Run"-Schlüssel überprüfen	Liefert Informationen zu Persistenztaktiken der Ransomware-Angreifer	Gängige Angriffsziele wie die „Run"- und „Startup"-Schlüssel auf neu erstellte Schlüssel oder Änderungen überprüfen	Baseline ermitteln → Netzwerkanalyse →
10	PERSISTENZ Nistet sich über ScheduledTasks ein	Neuerstellung geplanter Aufgaben überwachen	Liefert Informationen zu Persistenztaktiken der Ransomware-Angreifer	Windows-Ereignis ID 4698 ist ein Indikator dafür, dass eine neue geplante Aufgabe erstellt wurde	Baseline ermitteln → Netzwerkanalyse →
11	PERSISTENZ Nistet sich über WMI ein	Erstellung von WMI-Ereignis-Abonnements überwachen	Liefert Informationen zu Persistenztaktiken der Ransomware-Angreifer	Der Einsatz von Sysmon ermöglicht die Erkennung manipulierter WMI-Ereignisse. Standardmäßig verfügen die meisten Systeme nur über zwei vorkonfigurierte WMI-Abonnements.	Baseline ermitteln → Netzwerkanalyse →

	RANSOMWARE-TAKTIK / -TECHNIK	AKTIVE ABWEHR	WIRKUNG	KNIFFE, TIPPS, TRICKS UND EMPFEHLUNGEN	EINORDNUNG GEMÄSS MITRE ENGAGE
12	UMGEHEN VON ABWEHRMECHANISMEN Beendet Sicherheitsprozesse	Decoy-Sicherheitsprozesse zum Abfangen der Ransomware erstellen	Ermöglicht die Erkennung der Ransomware, wenn sie einen bekannten Sicherheitsprozess beendet	Decoy-Prozesse für gängige AVs erstellen, die Ransomware-Akteure gerne angreifen	Softwaremanipulation →
13	UMGEHEN VON ABWEHRMECHANISMEN Beendet Sicherheitsprozesse	• Registry auf beendete Sicherheitsservices überwachen • Decoys für Backup- und Datenbankservices erstellen • Beendung von Backup- und Datenbankservices überwachen	Warnt das Unternehmen, wenn Angreifer versuchen, wichtige Services zu deaktivieren	Bei Beendung von Services ändert sich der Startwert des entsprechenden Registry-Schlüssels auf 4 Decoys sollten für Services erstellt werden, die häufig angegriffen werden (u. a. Veeam, MSSQL und Oracle)	Softwaremanipulation → Analyse →
14	UMGEHEN VON ABWEHRMECHANISMEN Installiert eine ressourcenschonende Headless-VM	Headless-Starts für gängige VMs wie Virtual-Box, VMware und Hyper-V überwachen, um eine Baseline für Systeme zu erstellen, auf denen sie nicht installiert sein sollten	Ermöglicht die Erkennung von Techniken, die die Überprüfung durch EDR-Lösungen (Endpoint Detection and Response) umgehen	Datei-Hashes durch entsprechende Regeln zu Programmdateien zuordnen, die Headless-Starts zulassen; Prozessstarts für Befehlszeilenargumente überwachen	Baseline ermitteln → Netzwerkanalyse →
15	RECHTEERHÖHUNG Brute-Force-Diebstahl bzw. Wiederverwendung von Passwörtern für lokale Administratorkonten	• LAPS zum Schutz lokaler Administratorkonten einsetzen • Anmeldung für lokale Administratorkonten über das Netzwerk deaktivieren • Decoys von Anmeldedaten für lokale Administratorkonten in Antwortdateien erstellen	Eindämmung bzw. Beeinträchtigung der Auswirkungen der Wiederverwendung von Passwörtern für lokale Administratorkonten	Decoy-Passwörter in unattend.xml in einfügen, unter C:\Windows\Panther ablegen und auf Zugriffe überwachen	Köder → Sicherheitskontrollen → Operatives Ziel →
16	RECHTEERHÖHUNG Brute-Force-Diebstahl von Passwörtern für Domain-Administratorkonten (gilt auch für andere Konten mit hoher Berechtigungsstufe)	• Decoy für Domain-Administratorkonto erstellen • Domain-Administratorkonten sperren, sodass Nutzung nur über Domain-Controller möglich ist • Anmeldeversuche für Domain-Administratorkonto von nicht genehmigten Standorten überwachen	Schützt, erkennt und stört Ransomware-Angriffe auf Konten mit hoher Berechtigungsstufe	• Decoy-Konto erstellen und zu AD-Gruppen mit hoher Berechtigungsstufe hinzufügen • Anhand des Attributs logon-workstation kann die Anmeldung für Domain-Administratoren auf bestimmte Standorte beschränkt werden • Anmelde-Ereignisse 4624, 4625, 4768, 4771, 4776 überwachen	Köder → Operatives Ziel → Baseline ermitteln → Netzwerkanalyse →

	RANSOMWARE-TAKTIK / -TECHNIK	AKTIVE ABWEHR	WIRKUNG	KNIFFE, TIPPS, TRICKS UND EMPFEHLUNGEN	EINORDNUNG GEMÄSS MITRE ENGAGE
17	Rechteerhöhung Diebstahl von Anmeldedaten aus Browsern und Software	Decoy-Anmeldedaten als Köder platzieren, die den User zu Decoy-Systemen weiterleiten	Leitet die Ransomware zu einer gefälschten Angriffsfläche um; dadurch wird ihre Ausführung unterbrochen bzw. verlangsamt	Decoy-Anmeldedaten für Chrome, Edge, IE, Putty erstellen, die den User zu Decoy-Systemen und -Anwendungen umleiten Zusätzlich können diese Anmeldedaten mit Decoy-Konten aus dem Active Directory verknüpft werden	Köder →
18	Rechteerhöhung Diebstahl von Anmeldedaten aus dem Arbeitsspeicher	• Decoy-Anmeldedaten in CredMan und Arbeitsspeicher platzieren • Geschützte User-Gruppen für Konten mit hoher Berechtigungsstufe einrichten • Berechtigungen für Konten mit hoher Berechtigungsstufe sperren • Schutzmechanismen für LSASS	Verkleinert die Angriffsfläche für Diebstahl von Anmeldedaten für Konten mit hoher Berechtigungsstufe aus dem Arbeitsspeicher Erkennung über Decoy-Anmeldedaten verhindert Ransomware-Aktivitäten unter Nutzung der betreffenden Daten	Die Erstellung geschützter User-Gruppen bietet eine leistungsstarke Option, die Speicherung von Anmeldedaten im Arbeitsspeicher zu verhindern, hat jedoch einige betriebliche Nachteile, die abgewogen werden müssen. Empfiehlt sich für Konten mit hoher Berechtigungsstufe.	Operatives Ziel → Administratorzugriff → Köder → Sicherheitskontrollen →
19	Rechteerhöhung Versucht, Konten mit Rechten zur Erstellung von Gruppenrichtlinien zu kompromittieren	• Decoy-Konten mit GPO-Berechtigungen erstellen • Konten mit GPO-Rechten sperren, sodass die Anmeldung nur über den Domain Controller möglich ist • Gezielt nach Aktivitäten in GPO-Konten suchen, die von ungewöhnlichen Standorten ausgehen	Behindert die Ransomware bei der gezielten Suche nach GPO-Rechten durch Erkennen der Enumeration und Nutzung entsprechender Konten Verhindert die Weiterleitung von Anmeldedaten für GPO-Konten außerhalb von Domain-Controller-Systemen	Zur Erkennung der Enumeration von Decoy-Konten mit GPO-Rechten kann die Überprüfung verschiedener Konto-Attribute aktiviert werden Anhand des Attributs logonworkstation kann die Anmeldung für GPO-Administratoren auf bestimmte Standorte beschränkt werden	Operatives Ziel → Administratorzugriff → Köder → Sicherheitskontrollen → Netzwerkanalyse →
20	Rechteerhöhung Versucht, die SCCM-Administratorkonten zu kompromittieren	• Decoy-SCCM-Konten erstellen • Decoy-SCCM-Systeme mit Eintrag im Active Directory erstellen • Nutzung von SCCM-Konten auf bestimmte Server beschränken • Gezielt nach Aktivitäten in SSCM-Konten suchen, die von ungewöhnlichen Standorten ausgehen	Behindert die Ransomware bei der gezielten Suche nach SCCM-Rechten durch Erkennen der Enumeration und Nutzung entsprechender Konten bzw. Enumeration von SCCM-Servern		Operatives Ziel → Administratorzugriff → Köder → Sicherheitskontrollen → Netzwerkanalyse →

	RANSOMWARE-TAKTIK / -TECHNIK	AKTIVE ABWEHR	WIRKUNG	KNIFFE, TIPPS, TRICKS UND EMPFEHLUNGEN	EINORDNUNG GEMÄSS MITRE ENGAGE
21	RECHTEERHÖHUNG Active-Directory-Angriffe wie Kerberoasting	Kerberoasting-fähige Decoy-Konten erstellen	Stört die Abläufe von Angriffen auf Passwörter mit dem Ziel, Zugriff auf Anmeldedaten für Konten mit hoher Berechtigungsstufe zu erhalten	Decoy-Konten können durch Festlegen des SPN-Attributs Kerbe-roasting-fähig gemacht werden; zur Verhinderung von Brute-Force-Angriffen sollte das Passwort eine Länge von mindestens 30 Zeichen haben	Köder →
22	ZIELAUSWAHL Active-Directory-Angriffe wie Kerberoasting	Decoy-Systeme im DMZ-Segment hinzufügen	Nach einer erfolgreichen Erstinfizierung wird dadurch die Erkennung von Ransomware in der Erkundungsphase ermöglicht	Hinweis: Decoys mit Dateifreigaben müssen in der DMZ platziert werden.	Köder →
23	ZIELAUSWAHL Wählt Zielsysteme auf Rechnern mit Active Directory aus	• Decoy-Systeme im Active Directory erstellen und entsprechende Überwachung aktivieren, damit versuchte Enumera-tionen protokolliert werden • Baseline erstellen und entsprechen-de Überprüfungen aktivieren für alle Konten und Systeme, die Enumerationen des Active Directory durchführen	Mit einer Kombination aus Decoys und Baselining können versuchte Enumeratio-nen des Active Directory schnell erkannt und entspre-chende Maßnahmen ergriffen werden	• Decoy-Systeme in unterschiedlichen Organisationsein-heiten platzieren • Hostnamen für typische Angriffsziele wie „srv“ oder „server“ hinzufügen • Zur Erfüllung der Auswahlkriterien sollten Attribute wie Betriebssys-tem und Version hinzugefügt werden	Köder → Baseline ermitteln →
24	ZIELAUSWAHL Erkennt zugeordnete Laufwerke und Freigaben auf einem infizierten Host	Decoy-Anmeldedaten einrichten Decoy-Systeme erstellen, die Informatio-nen zu Freigaben enthalten	Die Ransomware wird bei Versuchen, auf dem Endgerät Enumeratio-nen und Scans durchzu-führen, stattdessen zu Decoy-Dateifreigaben umgeleitet.	CredMan ist ein beliebter Speicherort für Informationen über zugeordnete Freigaben Versteckte Laufwerke können in der Registry erstellt werden.	Köder →
25	ZIELAUSWAHL Erkennt Freigaben aus Active Directory	In Active Directory Decoy-Konten mit Datei-freigabe-Indikatoren in den Attributen erstellen	Die Ransomware wird bei Versuchen, über Active Directory Enumerationen durchzuführen, stattdessen zu Decoy-Dateifreigaben umgeleitet.	Zur Erkennung von Dateifreigaben werden Attribute wie profilepath, homedirectory und scriptpath analysiert.	Köder →
26	ZIELAUSWAHL Erkennt Subnetze aus im Active Directory angelegten Standor-ten und Subnetzen	Decoy-Subnetze mit Decoy-Systemen erstellen	Stört den Ablauf des Ransomware-Angriffs durch Umleiten auf Decoy-Netzwerke	Durch Hinzufügen einer Beschreibung wie „Kritisches Serverseg-ment“ wird das Subnetz Ransomware-Akteuren als attraktives Angriffs-ziel präsentiert	Köder → Netzwerkmanipulation →

	RANSOMWARE-TAKTIK / -TECHNIK	AKTIVE ABWEHR	WIRKUNG	KNIFFE, TIPPS, TRICKS UND EMPFEHLUNGEN	EINORDNUNG GEMÄSS MITRE ENGAGE
27	LATERALE BEWEGUNG Durchsucht das Netzwerk nach Ports mit lateralen Bewegungen — insbesondere 135, 445, 3389 und 5985/5986.	• Decoy-Systeme zu DMZ und wichtigen Serversegmenten hinzufügen • Durch Isolierung wird die segmentüber-greifende Erkennung von Ressourcen in DMZ und geschäfts-kritischen Serverseg-menten behindert. • Zwei-Faktor-Authentifizierung für Interaktionen mit geschäftskritischen Servern erzwingen • Gezielt nach Verbindungen zu diesen Ports suchen, die vom DMZ-Segment ausgehen	• Verhindert die laterale Ausbrei-tung von Ransomware in Bereiche, in denen die stärksten Auswirkungen auf die Geschäfts-tätigkeit zu erwarten sind • Zusätzlich wird die Erkennung der Ransomware bei Angriffsversuchen auf geschäftskriti-sche Ziele unterstützt	• Decoy-Systeme zur Erkennung von Ransomware in Kombination mit bestmöglicher Isolierung einset-zen, um die für Ransomware-Akteure exponierte Angriffsfläche zu minimieren • Durch Erstellen einer Baseline für den Traffic aus der DMZ an Ports, die laterale Bewe-gungen ermög-lichen, lassen sich Anomalien schnell erkennen	Köder → Isolierung → Netzwerkmanipulation → Netzwerkanalyse →
28	LATERALE BEWEGUNG Durchsucht das Netzwerk nach Datenbanken	• Decoy-Systeme mit Datenbanken zu DMZ und wichtigen Serversegmenten hinzufügen • Durch Isolierung wird die segmentüber-greifende Erkennung von Ressourcen in DMZ und geschäfts-kritischen Serverseg-menten behindert. • Baseline für Verbindungen aus dem DMZ-Segment ermitteln • Gezielt nach Verbin-dungen zu gängigen Datenbankservern suchen	• Verhindert die laterale Ausbrei-tung von Ransomware in Bereiche, in denen die stärksten Auswirkungen auf die Geschäfts-tätigkeit zu erwarten sind • Zusätzlich wird die Erkennung der Ransomware bei Angriffsversuchen auf geschäftskriti-sche Ziele unterstützt	• Decoy-Systeme zur Erkennung von Ransomware in Kombination mit bestmöglicher Isolierung einset-zen, um die für Ransomware-Akteure exponierte Angriffsfläche zu minimieren • Durch Erstellen einer Baseline für den Traffic aus der DMZ an Ports, die laterale Bewe-gungen ermög-lichen, lassen sich Anomalien schnell erkennen • Gezielt nach Verbindungen mit den Zielports 1433, 3306 und 1521 suchen	Köder → Vielfalt von Artefakten → Isolierung → Baseline ermitteln → Netzwerkanalyse →
29	LATERALE BEWEGUNG Verteilt die Payload für die Datenver-schlüsselung über SMB, z. B. PsExec	• Bestmögliche SMB-Blockierung • Decoy-Systeme für SMB-Interaktionen erstellen • Admin-Freigabe deaktivieren, damit Tools wie PsExec nicht ausge-führt werden können	• Durch bestmög-liche SMB-Blockierung wird Ransomware neutralisiert, die Payloads über SMB verteilt; dadurch lassen sich die Auswir-kungen von Ransomware erheblich reduzieren • Decoys ermögli-chen die Erkennung von Ransomware	Durch Blockieren eingehender SMB-Interaktionen zwischen Workstations wird die für Ransomware-Akteure exponierte Angriffsfläche minimiert	Köder → Isolierung → Administratorzugriff → Sicherheitskontrollen →

	RANSOMWARE-TAKTIK / -TECHNIK	AKTIVE ABWEHR	WIRKUNG	KNIFFE, TIPPS, TRICKS UND EMPFEHLUNGEN	EINORDNUNG GEMÄSS MITRE ENGAGE
30	LATERALE BEWEGUNG Verteilt die Payload für die Datenver-schlüsselung über GPO	Erstellung von Gruppen-richtlinien überwachen, insbesondere derjenigen, die geplante Aufgaben und Registryschlüssel verteilen	Benachrichtigungen über neu erstellte GPOs für die Verteilung von geplanten Aufgaben und Registry-Schlüsseln einrichten	Überwachung der GPO-Erstellung einrichten Optional kann die Überwachung des Richtlinienordners in C:\Windows\Sysvol\ sowie der Dateierstel-lung für ScheduledTask.xml und Registry.xml eingerichtet werden.	Baseline ermitteln → Überwachung der Systemaktivität →
31	LATERALE BEWEGUNG Verteilt die Payload für die Datenver-schlüsselung über SCCM oder andere Tools zur Software-bereitstellung	• Erstellung von SCCM-Richtlinien überwachen • SCCM-Richtlinien nach festem Zeitplan verteilen • Aktivitäten in SCCM-Konten verfolgen	Benachrichtigungen für SCCM-Richtlinien einrichten, die außer-halb der normalen Arbeitszeiten neu erstellt oder verteilt werden	Aktivitäten in SCCM-Konten über Win-dows-Ereignis ID 4768 und 4624 überwachen; dabei insbesondere auf Quelle der Anmeldung achten	Baseline ermitteln → Überwachung der Systemaktivität → Netzwerkanalyse →
32	CHECKLISTE FÜR VORVERSCHLÜSSE-LUNGSPHASE Beendet Debugger	Decoy-Prozess erstellen	Ermöglicht die Erken-nung der Ransomware, wenn ein Decoy-Prozess beendet wird	Gefälschten Prozess für windbg.exe und procmon.exe erstellen	Softwaremanipulation →
33	CHECKLISTE FÜR VORVERSCHLÜSSE-LUNGSPHASE Überprüft wechsel-seitige Ausschlüsse (Mutexes) zur Verhinderung erneuter Infektionen	Mutexes für kürzlich aufgetretene Ransomware löschen	Host wird dadurch zum ungeeigneten Angriffs-ziel für Ransomware	Sinnvoll bei akuter Bedrohung durch einen bestimmten Ransomware-Stamm	Pocket Litter →
34	CHECKLISTE FÜR VORVERSCHLÜSSE-LUNGSPHASE Vermeidet Infektio-nen, indem überprüft wird, ob der Betrieb in einer VM-Umge-bung erfolgt	Decoys für Registry-Schlüssel mit VM-Referenzen erstellen Decoys für Prozesse und Services erstellen, die mit VM-Umgebungen konsistent sind	Host wird dadurch zum ungeeigneten Angriffs-ziel für Ransomware	Prozessnamen wie vmware-vmx.exe verwenden	Köder → Pocket Litter → Softwaremanipulation →
35	CHECKLISTE FÜR VORVERSCHLÜSSE-LUNGSPHASE Beendet Datenbank- und MS-Office-Prozesse, um Datei-sperren zu vermeiden	Decoy-Prozesse für MS-Office-Produkte erstellen	Ermöglicht die Erken-nung der Ransomware, wenn sie einen Prozess beendet	Prozessnamen wie winword.exe und EXCEL.exe verwenden	Softwaremanipulation →
36	CHECKLISTE FÜR VORVERSCHLÜSSE-LUNGSPHASE Exfiltriert wichtige Dateien als Nachweis des unbefugten Zugriffs für Löse-geldforderungen	Decoy-Dateien erstellen, um Datenexfiltration zu erkennen	Die Erkennung von Datenexfiltrationen kann im Rahmen einer Abwehrstrategie als letztes Mittel eingesetzt werden. Dadurch können die durch einen laufenden Angriff verursachten Schäden begrenzt werden	Dateinamen wie pass-wörter.xls, assets.xls, sec-bericht.docx usw. hinzufügen	Köder → Pocket Litter →

	RANSOMWARE-TAKTIK / -TECHNIK	AKTIVE ABWEHR	WIRKUNG	KNIFFE, TIPPS, TRICKS UND EMPFEHLUNGEN	EINORDNUNG GEMÄSS MITRE ENGAGE
37	CHECKLISTE FÜR VORVERSCHLÜSSELUNGSPHASE • Löscht Volumenschattenkopien • Löscht Windows-Checkpoints durch Löschen aller Sicherungskopien mit wbadmin • Deaktiviert den Wiederherstellungsmodus in der Boot-Konfiguration mit bcdedit	Gezielt nach verdächtigen Prozesserstellungs- und Befehlszeilenargumenten suchen	Liefert Informationen über bevorstehende Infizierung des Hosts	Gezielt nach Prozessstarts durch vssadmin.exe, bcdedit.exe und wbadmin.exe suchen	Netzwerkanalyse → Überwachung der Systemaktivität →
38	VERSCHLÜSSELUNG Verschlüsselt Dateien mit gängigen Erweiterungen bzw. Erweiterungen, die auf wichtige Inhalte hindeuten	Decoys von Dateien erstellen, die Ransomware-Kriterien erfüllen	Die Erkennung von Datenexfiltrationen kann im Rahmen einer Abwehrstrategie als letztes Mittel zur Schadensbegrenzung eingesetzt werden	Erweiterungen wie .txt, .pdf, .pst, .bak usw. hinzufügen	Köder → Pocket Litter →
39	VERSCHLÜSSELUNG Dateierweiterung wird umbenannt	Dateierweiterung wird umbenannt	Die Erkennung von Datenexfiltrationen kann im Rahmen einer Abwehrstrategie als letztes Mittel zur Schadensbegrenzung eingesetzt werden	Überprüfung für Decoy-Datei einrichten und Regel zur Nachverfolgung von Protokollzeilen erstellen, in denen der Name der Decoy-Datei mit einer Erweiterung angegeben wird, die sich von der ursprünglich konfigurierten unterscheidet	Überwachung der Systemaktivität →
40	VERSCHLÜSSELUNG Folgt Symlinks, zugeordneten Laufwerken und Fileshares	Decoys für Symlinks, zugeordnete Laufwerke und Fileshares erstellen	Leitet Ransomware auf die gefälschte Angriffsfläche um, sodass die Auswirkungen auf das Unternehmen reduziert werden können	Symlink zum Desktop hinzufügen	Köder → Pocket Litter →

Schlussgedanken

Ransomware ist ein spannendes und hochaktuelles Thema. Jeder im Sicherheitsteam, vom CISO bis zum Analysten, sollte sich mit ihrer Funktionsweise vertraut machen und wissen, welche Strategien und Maßnahmen den Schaden am effektivsten begrenzen.

Und wie man im Ernstfall vorgeht. Die Gründe dafür liegen auf der Hand:

1. **Ransomware ist branchenunabhängig.**
2. **Ransomware kann mit allen Bereichen der IT-Umgebung interagieren — vom Perimeter über das interne Netzwerk, Endgeräten, Active Directory, Anwendungen bis hin zur Cloud.**
3. **Ransomware ist aktuell die einzige Gefahr, die den Geschäftsbetrieb komplett unterbrechen und ein Unternehmen zum Stillstand bringen kann.**

Ransomware-Angriffe stellen sämtliche Aspekte Ihres Sicherheitsprogramms auf den Prüfstein: Schutzmechanismen, Bedrohungserkennung, Vorfallbereitschaft und -reaktionen, Sicherheitslücken-Management, Compliance, Governance, Notfallwiederherstellung, User-Sensibilisierung, Fachkenntnisse und Kompetenzen, Kommunikation.

Der Zeit- und Arbeitsaufwand für den Aufbau einer aktiven Abwehrstrategie gegen Ransomware lohnt sich. Denn von den Auswirkungen eines Ransomware-Angriffs bleibt niemand verschont: weder der Vorstand oder die Aktionäre noch die Kunden, Auftragnehmer und Belegschaft Ihrer Organisation.

Zudem gibt es zahlreiche Überschneidungen und Ähnlichkeiten zwischen Ransomware-Taktiken und anderen Bedrohungsarten. Wenn es Ihnen also gelingt, eine effektive Strategie gegen Ransomware zu entwickeln, haben Sie gute Chancen, eine ganze Reihe akuter Herausforderungen in den Griff zu bekommen.

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Die Zscaler Zero Trust Exchange™ schützt tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlusten. Als weltweit größte Inline-Cloud-Sicherheitsplattform wird die SASE-basierte Zero Trust Exchange™ in über 150 Rechenzentren auf der ganzen Welt bereitgestellt. Weitere Informationen erhalten Sie auf **www.zscaler.com/de**. Auf X (ehemals Twitter) finden Sie uns unter **@zscaler**.

+1 408 533 0288 Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA zscaler.com/de

zscaler™

Zero Trust Everywhere