

KURZFASSUNG FÜR FÜHRUNGSKRÄFTE

Acronis TRU Cyber Pulse 2026

Die wichtigsten Erkenntnisse und ihre Auswirkungen auf die IT-Sicherheit

Acronis
Threat Research Unit

Das Wichtigste im Überblick



Cyberangriffe entwickeln sich in einer Weise weiter, die sowohl die Geschwindigkeit als auch die Reichweite von Systemeinbrüchen erhöht.

Immer mehr Bedrohungsakteure setzen KI-Agenten ein, um Angriffs-Workflows zu automatisieren. Darüber hinaus nutzen sie gestohlene Identitäten, um sich zwischen miteinander verbundenen Services zu bewegen, und nehmen Sicherheitskontrollen ins Visier, um die Fähigkeiten zur Erkennung von Angriffen und zur Wiederherstellung von Systemen zu schwächen.

Die erste Ausgabe des Sicherheitsberichts „Acronis TRU Cyber Pulse 2026“ bündelt die Untersuchungen der Acronis Threat Research Unit (TRU) zu neu aufkommenden Angriffstechniken sowie zu Spionageaktivitäten und Cyberkriminalität. Die Ergebnisse lassen ein gemeinsames Muster erkennen: Eine anfängliche Kompromittierung kann einen Zugang eröffnen, der weit über das betroffene Gerät oder Benutzerkonto hinausreicht.

Für MSPs (Managed Service Provider) entstehen dadurch besondere Risiken. Wird eine Identität mit administrativen Berechtigungen, ein Tool für die Remote-Verwaltung oder ein gemeinsam genutzter Service kompromittiert, kann dies mehrere Kundenumgebungen gefährden. Unternehmen müssen daher nicht nur verstehen, wie Cyberkriminelle sich Zugang verschaffen, sondern auch, wie weit dieser Zugang reichen kann.

Sechs Erkenntnisse kennzeichnen die in diesem Bericht untersuchte Bedrohungslage.

1. KI-Agenten vergrößern das Ausmaß von Cyberangriffen

Viele Bedrohungsakteure setzen KI inzwischen nicht mehr nur für einzelne Aufgaben ein, etwa um Phishing-Nachrichten zu verfassen oder Schwachstellen zu analysieren. Einige von ihnen integrieren große Sprachmodelle (LLMs) mit Messaging-Plattformen und Tools für Offensive Security. Dabei nutzen sie ein persistentes Gedächtnis, um den Kontext beizubehalten und umfassendere Angriffsoperationen zu koordinieren.

Die BOSSAI-Untersuchung der Acronis TRU veranschaulicht diese Entwicklung. Eine einzelne Person verband mehr als 10 Modelle mit Angriffs-Frameworks und der dazugehörigen Infrastruktur. Auf diese Weise konnte die Person Ziele in mehreren Ländern koordiniert ausspähen, deren Schwachstellen ausnutzen und die Angriffsinfrastruktur verwalten.

Diese Ergebnisse zeigen, wie agentische Systeme den manuellen Aufwand verringern können, der für die Durchführung komplexer Angriffsoperationen erforderlich ist.

Die Einführung von KI bringt zudem neue Angriffsflächen mit sich. Die TRU identifizierte mehr als 575 schädliche Skills (Erweiterungen) für den KI-Agenten OpenClaw, verteilt auf 13 Entwicklerkonten. Diese Pakete gaben sich als legitime Tools aus, schleusten dabei jedoch Malware ein.

```
export ANTHROPIC_SMALL_FAST_MODEL="MiniMax-M3"
export ANTHROPIC_DEFAULT_SONNET_MODEL="MiniMax-M3"
export ANTHROPIC_DEFAULT_OPUS_MODEL="MiniMax-M3"
export ANTHROPIC_DEFAULT_HAIKU_MODEL="MiniMax-M3"
claude
export ANTHROPIC_BASE_URL="https://api.minimaxi.com/anthropic"
export ANTHROPIC_AUTH_TOKEN="sk-cp-[redacted]"
export API_TIMEOUT_MS="3000000"
export CLAUDE_CODE_DISABLE_NONESSENTIAL_TRAFFIC=1
export ANTHROPIC_MODEL="MiniMax-M3"
export ANTHROPIC_SMALL_FAST_MODEL="MiniMax-M3"
export ANTHROPIC_DEFAULT_SONNET_MODEL="MiniMax-M3"
export ANTHROPIC_DEFAULT_OPUS_MODEL="MiniMax-M3"
export ANTHROPIC_DEFAULT_HAIKU_MODEL="MiniMax-M3"
claude --model MiniMax-M3
export ANTHROPIC_BASE_URL="https://api.minimaxi.com/anthropic"
```

Claude Code, umgeleitet über MiniMax.

Auswirkungen auf die IT-Sicherheit:

Unternehmen müssen KI-Agenten und die damit verbundenen Tools als privilegierte Systeme behandeln. Die Berechtigungen der KI-Agenten, externe Skills, Anmeldedaten und Netzwerkzugriffe erfordern unabhängige Sicherheitskontrollen und ein unabhängiges Monitoring.

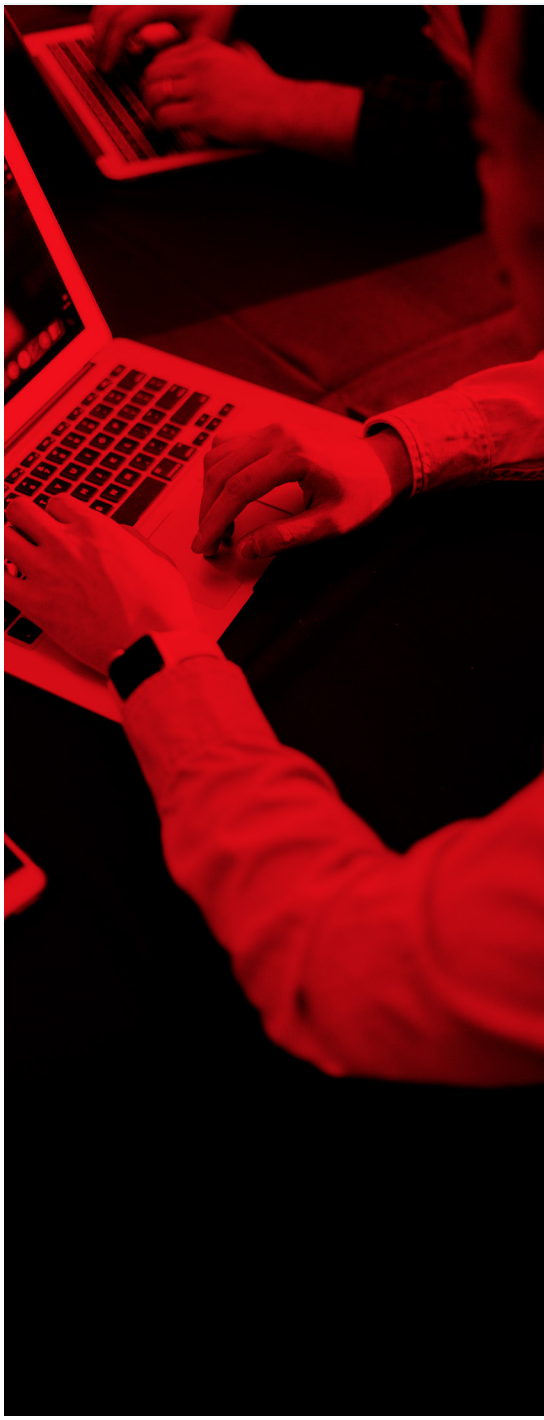
2. Gestohlene Identitäten entwickeln sich zu einem Hauptweg für weitreichende Kompromittierungen

Infostealer (Schadsoftware zum Diebstahl von Daten) und identitätsbezogene Angriffe zielen zunehmend auf Anmeldedaten, Authentifizierungstokens, Browser-Sitzungen und Zugänge zu Cloud-Services ab.

Mit diesen Informationen können Cyberkriminelle auf verbundene Applikationen und Services zugreifen, teilweise ohne dass eine erneute Abfrage der Multi-Faktor-Authentifizierung (MFA) ausgelöst wird. Gestohlene Zugänge können zudem an andere Bedrohungsakteure weitergegeben oder verkauft werden, darunter Ransomware- und Spionagegruppen.

Das Risiko erstreckt sich auch auf Entwicklungsumgebungen. Bei aktuellen Untersuchungen wurde Malware identifiziert, die auf API-Schlüssel für KI-Services, Anmeldedaten für Repositories und weitere Secrets (vertrauliche Daten zur Authentifizierung) in der Software-Entwicklung abzielt. Diese Anmeldedaten können Zugang zu weiteren Systemen und Projekten verschaffen.

Bei MSPs sind privilegierte Identitäten für Cyberkriminelle besonders wertvoll, weil diese Identitäten unter Umständen Zugang zu mehreren Kundenumgebungen verschaffen.



Auswirkungen auf die IT-Sicherheit:

Es reicht nicht aus, Malware zu entfernen oder ein Kennwort zurückzusetzen. Vielmehr müssen bei der Reaktion auf einen Vorfall auch betroffene Sitzungen widerrufen, Anmeldedaten rotiert, Änderungen an Authentifizierungseinstellungen überprüft und verbundene Services untersucht werden.

3. Cyberkriminelle schwächen gezielt Sicherheits- und Wiederherstellungsmechanismen

Die Deaktivierung von Sicherheits-Tools ist zu einem wichtigen Bestandteil moderner Systemeinbrüche geworden.

Im April 2026 wurde „Defense Impairment“ (Beeinträchtigung von Abwehrmechanismen) als eigenständige Taktik in das MITRE ATT&CK-Framework aufgenommen. Die Taktik umfasst gezielte Eingriffe in Abwehrsysteme.

Die Untersuchungen der Acronis TRU zu Ransomware-Gruppen, darunter Qilin und The Gentlemen, zeigen, wie Cyberkriminelle Prozesse von Sicherheitssoftware beenden, das Monitoring beeinträchtigen und Wiederherstellungsmechanismen stören können.

Diese Aktivitäten können den Überblick der Sicherheitsteams einschränken, während sich Cyberkriminelle durch Netzwerke bewegen, Informationen stehlen oder die Verschlüsselung von Systemen vorbereiten.

Besonders groß ist das Risiko, wenn Cyberkriminelle die Kontrolle über Management-Server oder Administratorkonten erlangen, die in mehreren Umgebungen genutzt werden.



Desktop-Hintergrundbild der Gruppe „The Gentlemen“

Auswirkungen auf die IT-Sicherheit:

Unternehmen sollten unabhängig überwachen, in welchem Zustand sich ihre Sicherheits-Agenten befinden, ob die Protokollierung geändert wird und ob versucht wird, den Schutz zu deaktivieren. Die Backup-Administration muss von der routinemäßigen Systemadministration getrennt bleiben. Zudem müssen Wiederherstellungs-prozesse anhand von Szenarien getestet werden, in denen Anmeldedaten oder Infrastrukturen kompromittiert sind.

4. Vertrauenswürdige Services und Software werden missbraucht, um Angriffe zu verschleiern

Gängige Plattformen, darunter GitHub, Telegram und Cloud-Storage-Services, werden zunehmend von Cyberkriminellen und Spionagegruppen genutzt, um Malware zu verbreiten oder die Kommunikation mit kompromittierten Systemen aufrechtzuerhalten.

Da diese Services auch legitimen geschäftlichen Zwecken dienen, ist schädlicher Datenverkehr oft nur schwer von einer autorisierten Nutzung zu unterscheiden.

Bei Untersuchungen der Acronis TRU wurden die Verbreitung von Malware über GitHub-Repositories und die Nutzung vertrauenswürdiger Cloud-Services für die Fernsteuerung kompromittierter Systeme (Command and Control) dokumentiert.

Die TamperedChef-Kampagne zeigte eine weitere Schwäche herkömmlicher Vertrauensmerkmale. Die Cyberkriminellen hinter der Kampagne verbreiteten funktionsfähige schädliche Applikationen mit gültigen Code-Signatur-Zertifikaten. Das zeigt, dass eine legitime Signatur noch nicht belegt, dass Software sicher ist.

Auswirkungen auf die IT-Sicherheit:

Unternehmen sollten die Aktivitäten von Applikationen und Services im Kontext bewerten, statt sich ausschließlich auf die Domain-Reputation oder digitale Signaturen zu verlassen. Unerwartete Downloads, Aktivitäten über Cloud-APIs und Verbindungen zur Remote-Verwaltung müssen auch dann untersucht werden, wenn gängige Services daran beteiligt sind.



5. Ransomware-Gruppen passen sich an Störungen an und dehnen ihre Angriffe über Windows hinaus aus

Maßnahmen der Strafverfolgungsbehörden können die Infrastruktur von Cyberkriminellen stören. Die Tools und das Fachwissen hinter den kriminellen Aktivitäten können jedoch weiterhin verfügbar bleiben.

Wie die Forschung der Acronis TRU zeigt, können sich kriminelle Gruppen neu organisieren und ihre Aktivitäten unter anderen Namen fortsetzen. Möglich machen das Ransomware-Affiliates (Akteure, die die Tools und die Infrastruktur von Ransomware-Gruppen nutzen), geleakter Quellcode und gemeinsam genutzte Angriffstechniken.

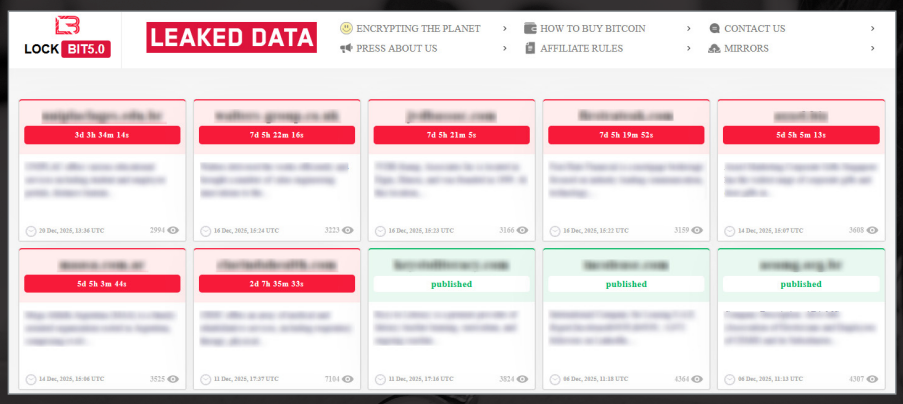
Auch das technische Spektrum von Ransomware wird breiter.

LockBit 5.0 umfasst Varianten für Windows, Linux und VMware ESXi. Die Ransomware-Gruppe INC hat bereits gezeigt, dass sie Linux- und ESXi-Umgebungen angreifen kann. Qilin wiederum hat das Windows-Subsystem für Linux (WSL) genutzt, um ein Linux-Verschlüsselungsprogramm unter Windows auszuführen.

Greifen Cyberkriminelle Virtualisierungsinfrastrukturen an, können sie mehrere Workloads beeinträchtigen und Systeme treffen, die für die Wiederaufnahme des Geschäftsbetriebs unverzichtbar sind.

Auswirkungen auf die IT-Sicherheit:

Die Schutzmaßnahmen gegen Ransomware müssen Linux-Hosts, Hypervisoren und die Systeme zur Verwaltung virtueller Maschinen abdecken. Unternehmen sollten das unerwartete Herunterfahren virtueller Maschinen und das Löschen von Snapshots überwachen. Zugleich sollten sie sicherstellen, dass die Wiederherstellungsinfrastruktur auch während einer Kompromittierung zugänglich bleibt.



Leak-Website von LockBit 5.0

6. Die Ausnutzung von Schwachstellen und Vertrauensbeziehungen vergrößert die Reichweite von Systemeinbrüchen

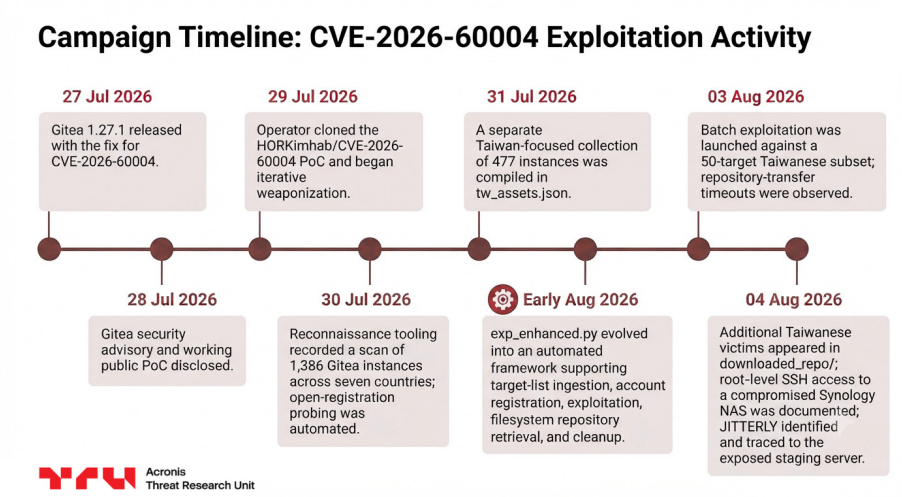
Neu veröffentlichte Schwachstellen werden von Cyberkriminellen schnell ausgenutzt. Damit bleibt Unternehmen weniger Zeit, um Sicherheits-Updates bereitzustellen.

In der Red Heron-Untersuchung passten die Cyberkriminellen kurz nach dem Bekanntwerden einer kritischen Schwachstelle in Gitea einen öffentlich verfügbaren Exploit an. Auf den kompromittierten Entwicklungsservern waren Repositories und Anmeldedaten zugänglich, die für weitere Systemeinbrüche genutzt werden konnten.

Untersuchungen zu Spionageaktivitäten ließen ein ähnliches Muster erkennen: Vertrauensbeziehungen werden von Bedrohungsakteuren zunehmend ausgenutzt, um Ziele auf indirektem Weg zu erreichen.

IT-Dienstleister, Entwicklungsumgebungen und Infrastrukturen für die Software-Verteilung können Zugang zu Unternehmen verschaffen, die Cyberkriminelle nicht ohne Weiteres direkt kompromittieren können.

Für MSPs haben solche Angriffe besonders schwerwiegende Folgen, weil schon die Kompromittierung eines einzigen Services oder einer einzigen Identität mehrere Kundenumgebungen gefährden kann.



Auswirkungen auf die IT-Sicherheit:

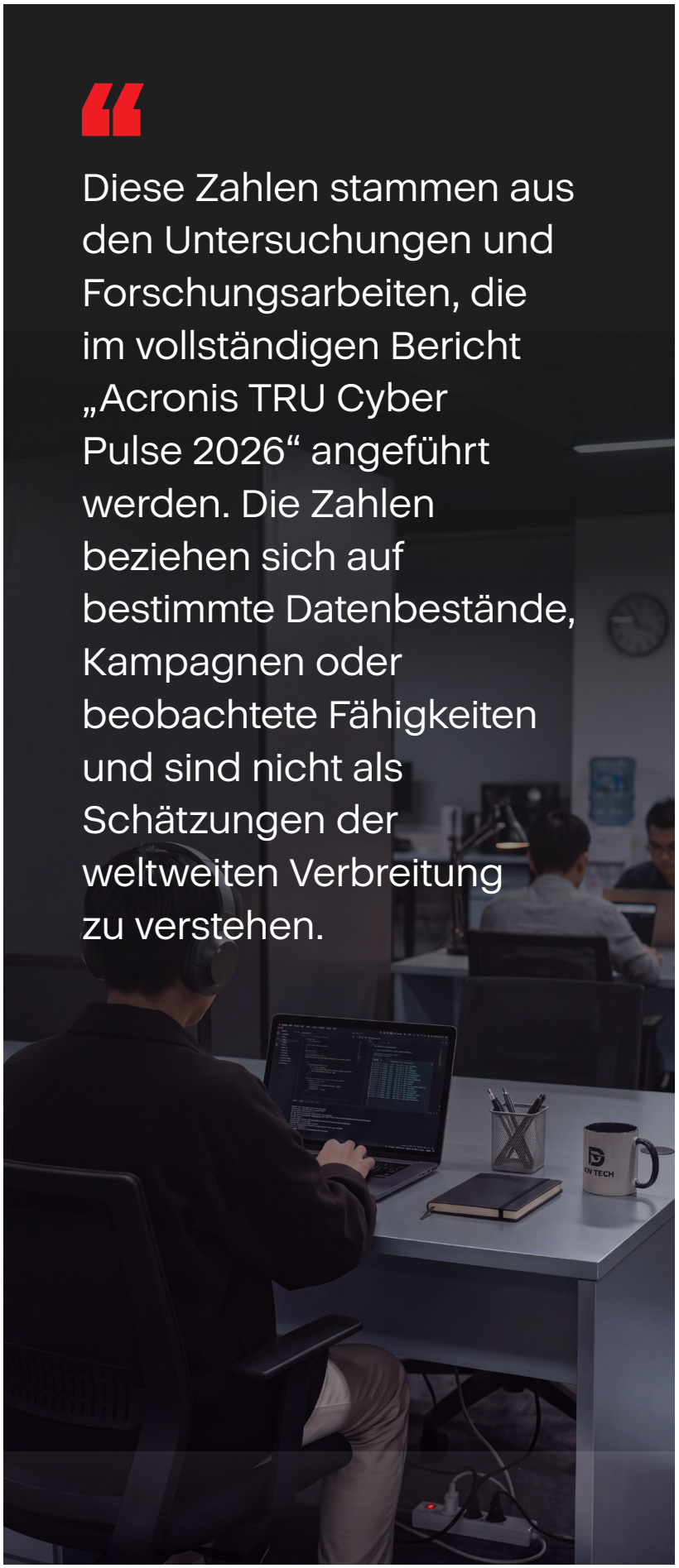
Bei der Behebung von Schwachstellen ist nicht nur deren Schweregrad zu berücksichtigen, sondern auch, welchen Zugang das betroffene System verschafft. Nach der Ausnutzung einer Schwachstelle müssen Unternehmen untersuchen, ob Persistenzmechanismen eingerichtet wurden, ob Anmeldedaten gestohlen wurden und welche Aktivitäten in den verbundenen Umgebungen stattgefunden haben.

Forschungsergebnisse im Überblick

Die folgenden ausgewählten Ergebnisse veranschaulichen das Ausmaß der Aktivitäten, die im vollständigen Bericht dokumentiert sind.

Forschungsergebnis | Belege

- **KI-gestützter Angriff:** Im Fall BOSSAI wurden mehr als 10 KI-Modelle mit Angriffs-Tools und der dazugehörigen Infrastruktur verbunden.
- **Bedrohungen über die KI-Lieferkette:** Die TRU identifizierte mehr als 575 schädliche OpenClaw-Skills, verteilt auf 13 Entwicklerkonten.
- **Gefährdung durch Remote-Zugriff:** Bei einer Analyse von mehr als 1,8 Millionen Endpunkten mit Acronis RMM war auf 63,1 % dieser Endpunkte mindestens ein weiteres RMM- oder Remote-Zugriffs-Tool installiert.
- **Verzögerungen bei der Patch-Installation:** Laut der TRU lag die Zeit bis zur Installation von Patches für Applikationen von Drittanbietern im zweiten Halbjahr 2025 im Median bei 5,7 Tagen.
- **Ausweitung von Ransomware-Angriffen:** LockBit 5.0 umfasst Varianten für Windows-, Linux- und ESXi-Umgebungen.



> Diese Zahlen stammen aus den Untersuchungen und Forschungsarbeiten, die im vollständigen Bericht „Acronis TRU Cyber Pulse 2026“ angeführt werden. Die Zahlen beziehen sich auf bestimmte Datenbestände, Kampagnen oder beobachtete Fähigkeiten und sind nicht als Schätzungen der weltweiten Verbreitung zu verstehen.

Prioritäten für mehr Cyber-Resilienz



Aus den Ergebnissen lassen sich fünf praxisnahe Prioritäten für MSPs und Unternehmen ableiten, die die Auswirkungen von Cyberangriffen verringern wollen.

1. Begrenzen Sie die Reichweite kompromittierter Identitäten. Setzen Sie eine Phishing-resistente Authentifizierung ein, schränken Sie privilegierte Zugriffe ein und behalten Sie den Überblick über Sitzungen, Applikationsberechtigungen und Verbindungen zur Remote-Verwaltung.

2. Priorisieren Sie Schwachstellen danach, wie stark das betroffene System exponiert ist und welchen Zugang es verschafft. Beschleunigen Sie die Behebung von Schwachstellen in Systemen, die über das Internet erreichbar sind, und in administrativen Systemen, insbesondere in solchen, die Anmeldedaten enthalten oder Zugang zu anderen Umgebungen verschaffen. Untersuchen Sie nach einer vermuteten Ausnutzung von Schwachstellen, ob Persistenzmechanismen eingerichtet und Anmeldedaten offengelegt wurden.

3. Erkennen Sie Versuche, den Schutz zu deaktivieren. Überwachen Sie Ausfälle von Sicherheits-Agenten, unerwartete Aktivitäten von Treibern und Änderungen an den Einstellungen für die Protokollierung oder den Schutz. Behandeln Sie ungeklärte Lücken im Monitoring privilegierter Systeme als mögliche sicherheitsrelevante Vorfälle.

4. Schützen Sie geschäftskritische Infrastrukturen und Wiederherstellungsfähigkeiten. Weiten Sie das Monitoring auf Linux-, Virtualisierungs- und Backup-Umgebungen aus. Trennen Sie die Berechtigungen für Wiederherstellungen von der routinemäßigen Administration und testen Sie Ihre Wiederherstellungsprozesse auch für den Fall, dass die regulären Verwaltungssysteme nicht verfügbar sind.

5. Legen Sie Sicherheitsgrenzen für KI-Agenten fest. Inventarisieren Sie die Frameworks für KI-Agenten, die damit verbundenen Tools und die externen Skills. Schränken Sie deren Berechtigungen ein, setzen Sie eine Trennung zwischen den einzelnen Kundenumgebungen durch und verlangen Sie für Aktionen mit weitreichenden Folgen eine unabhängige Genehmigung.

Diese Prioritäten verfolgen ein gemeinsames Ziel: den für Cyberkriminelle verfügbaren Zugang zu begrenzen, dessen Missbrauch zu erkennen und die Fähigkeit zu erhalten, wesentliche Services wiederherzustellen.

Fazit:
Cyber-Resilienz hängt davon ab, systemübergreifende Zugänge unter Kontrolle zu halten

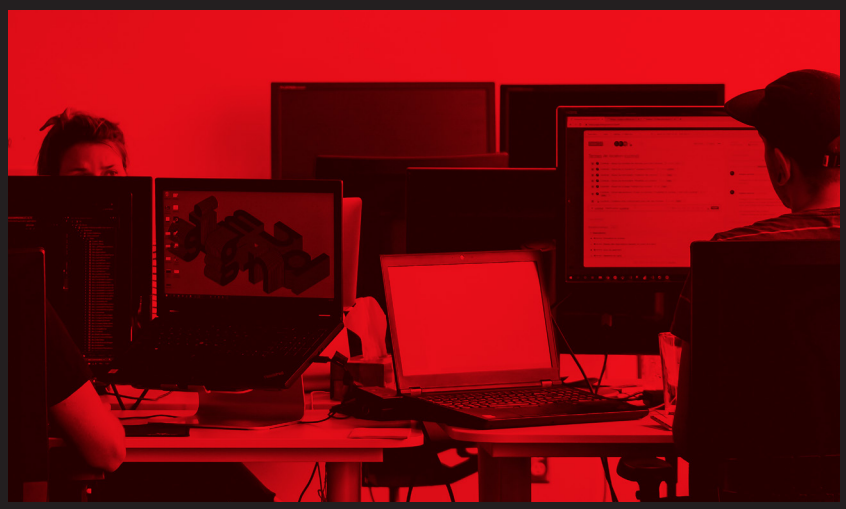
Die Bedrohungslage im Jahr 2026 wird nicht nur von neuen Angriffstechniken geprägt, sondern auch davon, dass Bedrohungsakteure die Verbindungen zwischen Identitäten, Services und Infrastrukturen ausnutzen können.

KI-Agenten können etablierte Angriffs-Workflows beschleunigen. Gestohlene Anmeldedaten können einen Zugang verschaffen, der über Cloud-Applikationen und Kundenumgebungen hinweg reicht. Ransomware-Gruppen können Sicherheitskontrollen beeinträchtigen und die Infrastruktur ins Visier nehmen, die für die Wiederherstellung benötigt wird.

Für MSPs und IT-Verantwortliche besteht die zentrale Herausforderung darin, die Reichweite einer Kompromittierung zu verstehen und diese einzudämmen, bevor Cyberkriminelle weitere Systeme kompromittieren können.

Unternehmen, die den Überblick über Identitäten, Endpunkte, Cloud-Services und die Wiederherstellungsinfrastruktur behalten, sind besser aufgestellt, um unbefugte Aktivitäten zu erkennen, Vorfälle einzudämmen und geschäftskritische Betriebsabläufe wieder aufzunehmen.

Lesen Sie den vollständigen Bericht „Acronis TRU Cyber Pulse 2026“ mit ausführlichen Untersuchungen, technischen Erkenntnissen und weiteren Sicherheitsempfehlungen.



Über diese Forschungsarbeit

Der Bericht „Acronis TRU Cyber Pulse 2026“ führt Untersuchungen zu aktuellen Bedrohungen, Malware-Analysen, Forschungsarbeiten zu Angriffskampagnen und relevante Telemetriedaten von Acronis zusammen. Der Bericht untersucht neu aufkommende Angriffstechniken sowie Aktivitäten im Zusammenhang mit hochentwickelten permanenten Bedrohungen (APTs) und Cyberkriminalität. Ein besonderes Augenmerk liegt dabei auf den Auswirkungen für MSPs und ihre Kundenunternehmen.

Autor:innen



Santiago Pontiroli,
Leiter der Threat Intelligence-Forschung



Alexander Ivanyuk,
Senior Director, Technology

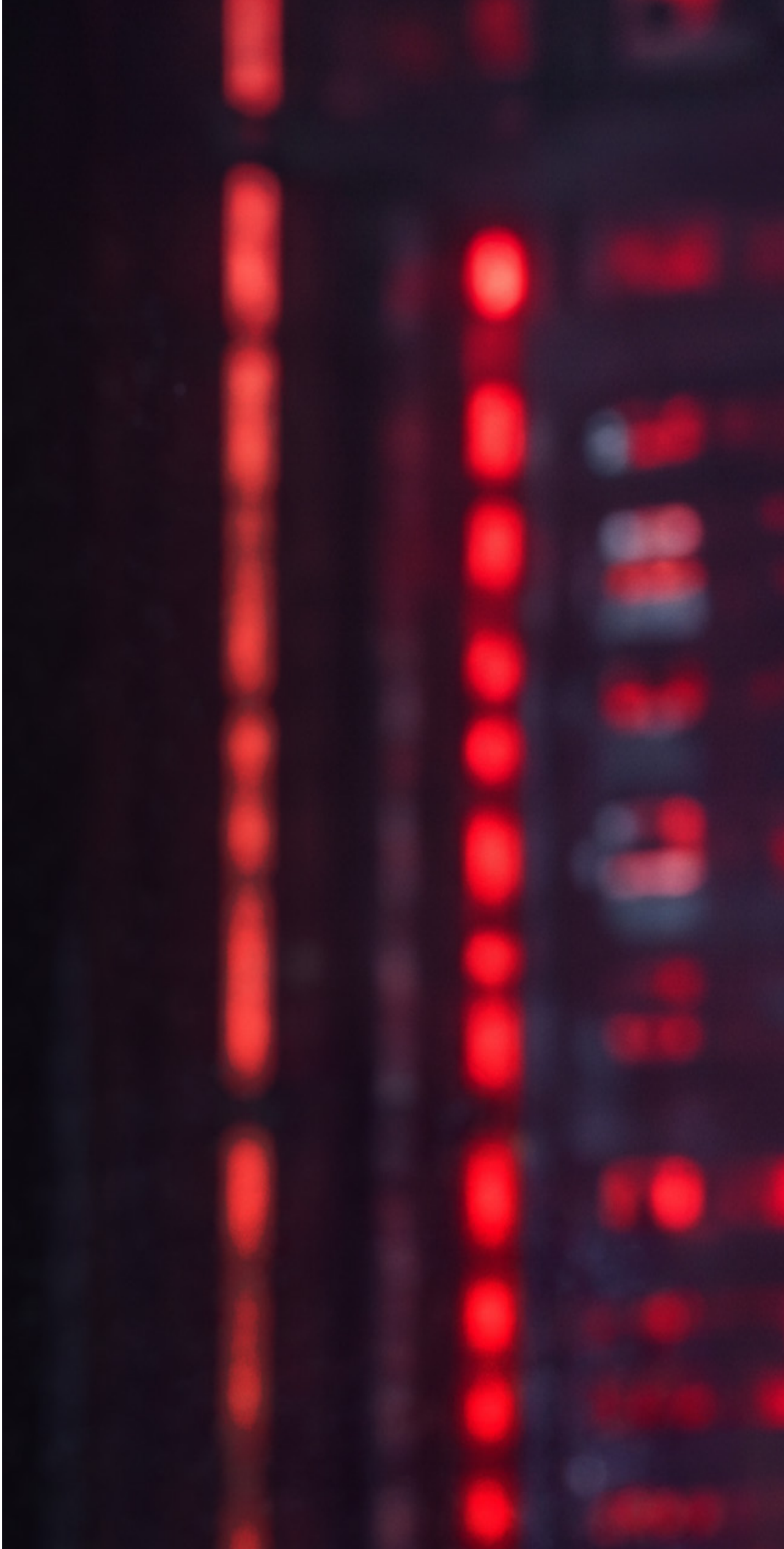


Eliad Kimhy,
Senior-Forscher bei der TRU



Subhajeet Singha,
Senior-Forscher bei der TRU

Acronis
Threat Research Unit



Copyright © 2003–2026 Acronis International GmbH. Alle Rechte vorbehalten. Acronis und das Acronis Logo sind eingetragene Markenzeichen der Acronis International GmbH in den Vereinigten Staaten und/oder in anderen Ländern. Alle anderen Marken oder eingetragenen Marken sind das Eigentum ihrer jeweiligen Inhaber. Technische Änderungen, Abweichungen bei den Abbildungen sowie Irrtümer sind vorbehalten.

2026