kaspersky BRING ON THE FUTURE

Kaspersky Threat Intelligence

Anwendungsfälle strategischer Threat Intelligence

Lange Zeit war die gängige Meinung, dass eine passive Strategie – der Schutz des Netzwerkperimeters und Workstations – ausreichend ist. Da Unternehmen immer häufiger das Ziel von ausgefeilten und zielgerichteten Angriffen werden, Umfassender Schutz muss über neue Methoden bereitgestellt werden, die auf Bedrohungsinformationen basieren.
Diese Informationen bereitzuhalten, erfordert viel Mühe und ein hohes Maß an Fachwissen. Mit Petabytes an aussagekräftigen Bedrohungsdaten und einem Pool weltweit agierender Experten unterstützt Kaspersky Unternehmen dabei, die Immunität gegen Cyberangriffe aufrechtzuerhalten.

Wer die Risiken versteht, kann informierte Entscheidungen treffen, wenn beispielsweise eine neue Initiative gestartet, eine neue Zweigniederlassung eröffnet oder ein Investment in neue Technologien geplant wird. Außerdem können so Eindämmungsstrategien besser proaktiv entwickelt und dazugehörige Budget- und Personalanforderungen gerechtfertigt werden.

Wir sind vom Internet abhängig. Die geringen Kosten und das hohe Tempo der Kommunikation über das Internet machen es zu einem festen Bestandteil des Fundaments erfolgreicher Unternehmen und Regierungen. Dynamische und miteinander verbundene Umgebungen bieten verschiedene wichtige Funktionen mit Möglichkeiten zur Verbesserung der Kommunikation, zum Schutz personenbezogener, vertraulicher und anderer Daten und für eine Beaufsichtigung und Kontrolle kritischer Systeme und Geschäftsprozesse. Allerdings vergrößert eine stets zunehmende Interkonnektivität die Angriffsfläche, denn Angreifer nutzen jede mögliche Schwachstelle, die sich ihnen bietet.

Seit einigen Jahren verschwimmen die Grenzen zwischen den verschiedenen Bedrohungsarten und den verschiedenen Arten von Bedrohungsakteuren. Ein Beispiel dafür ist das Code-Dumping der Gruppe Shadow Brokers, die hochentwickelte Exploits kriminellen Vereinigungen anbietet, die andernfalls keinen Zugang zu derart komplexen Codes haben würden. Ein Beispiel dafür ist das Aufkommen von APT-Kampagnen, die nicht auf Cyberspionage, sondern auf Diebstahl ausgerichtet sind – um an Geld zu kommen, mit dem andere Aktivitäten der APT-Gruppe finanziert werden sollen.

Die Motivationen von Bedrohungsakteuren sind sehr unterschiedlich – von Gelddiebstahl über die Schwächung der Konkurrenz bis hin zu Identitätsdiebstahl und Betrug. Außerdem haben alle Branchen und Unternehmen ihre eigenen Daten, die es zu schützen gilt, sowie ganz individuelle Programme und Technologien, mit denen sie arbeiten. All das führt dazu, dass die Angriffe auf sehr unterschiedliche Weise ausgeführt werden können – und jeden Tag entstehen neue Methoden.

In dieser sich schnell verändernden Bedrohungslandschaft kann die Ankurbelung des geschäftlichen Wachstums durch den digitalen Wandel eine große Herausforderung darstellen. Dabei müssen die Geschäftsführungen einen strategischen Ansatz verfolgen, indem sie Cyberrisiken stets gegen die allgemeinen geschäftlichen Ziele und Prioritäten abwägen.

Strategische Threat Intelligence bietet eine umfassende Sicht auf die Angriffstrends, Techniken und Methoden, die von Angreifern angewendet werden – einschließlich ihrer Motivationen und Attributionen. Außerdem können so bestimmte Fragen leichter beantwortet werden:

- Wer sind Ihre Gegner? Welches Ziel verfolgen sie?
- Welche Bedrohungsgruppen sind in Ihrer Branche oder Region aktiv?
- Genutzte Angriffsvektoren
- Was wäre die effektivste Methode, einen Angriff gegen Ihr Unternehmen zu starten?
- Welche Routen und welche Informationen kann ein Angreifer nutzen, der es speziell auf Sie abgesehen hat?
- Hat der Angriff bereits stattgefunden? Sind Sie gefährdet?
- Welche Maßnahmen sind erforderlich, um das Risikoprofil zu verringern?

Wenn Sie die Antworten auf diese Fragen Ihren kritischen Assets, Systemen und Geschäftsprozessen zuordnen, können Sie eine gründliche Risikoanalyse durchführen. Des Weiteren können Sie den Führungskräften klare, relevante Risikoszenarien kommunizieren – und dabei Investitionen in spezielle Programme, Technologien und Mitarbeiter rechtfertigen. Dank dieser Einblicke können Sie Ihre Verteidigungsstrategie auf genau die Bereiche konzentrieren, die als Hauptziele der Cyberkriminellen identifiziert wurden. Auf diese Weise handeln Sie schnell und präzise und minimieren das Risiko eines erfolgreichen Angriffs.

Das Angebot von Kaspersky

Berichtsart	Gelieferte Informationen	Anwendungsfall
APT Intelligence Reporting	• Beschreibungen der Taktiken und Methoden, die von Angreifern in Cyberspionage-Kampagnen mit branchenübergreifender Ausrichtung eingesetzt werden • Profile von Bedrohungsakteuren mit den von ihnen angewandten Taktiken, Techniken und Abläufen (Tactics, Techniques and Procedures, TTPs) • Zuordnung der dazugehörigen TTPs zu MITRE ATT&CK – eine Wissensdatenbank mit TTPs basierend auf realen Erfahrungen	• Verstehen Sie die Bedrohungsakteure, die Ihre Branche oder Ihre Region ins Visier genommen haben, und welche TTPs sie einsetzen • Ermitteln Sie, welche Informationsbestände und Systeme einem Risiko ausgesetzt sind, die potenziellen Gefährdungsfolgen und die entsprechende Priorisierung • Passen Sie Ihre Informationssicherheitsstrategien an, planen und rechtfertigen Sie Investments in bestimmte Technologien, Mitarbeiter und Programme, die potenzielle Angriffsvektoren abdecken
Financial Threat Intelligence Reporting	• Beschreibungen der Taktiken und Methoden, die von Angreifern eingesetzt werden, die den Finanzsektor anvisieren • Informationen über Angriffe auf konkrete Infrastrukturen, wie Geldautomaten oder Point-of-Sale-Geräte • Informationen über spezifische Tools, die auf Finanznetzwerke zugeschnitten sind, die von Cyberkriminellen in Darknet-Communities und Foren in verschiedenen Regionen verwendet, entwickelt und verkauft werden	• Ermitteln Sie die Angreifer von Finanzinstituten weltweit und die von ihnen eingesetzten TTPs • Ermitteln Sie, welche Informationsbestände und Systeme einem Risiko ausgesetzt sind, die potenziellen Gefährdungsfolgen und die entsprechende Priorisierung • Passen Sie Ihre Informationssicherheitsstrategien an, planen und rechtfertigen Sie Investments in bestimmte Technologien, Mitarbeiter und Programme, die potenzielle Angriffsvektoren abdecken
Digital Footprint Intelligence	• Passive Identifizierung des Netzwerkperimeters, der verfügbaren Services und der bestehenden Schwachstellen • Individuelle Schwachstellen- und Exploit-Analyse • Ermittlung, Überwachung und Analyse aktiver oder inaktiver Malware-Proben, die Ihr Unternehmen ins Visier genommen haben • Offengelegte Anmelde- und andere Daten • Phishing-Bedrohungen, die Kunden ins Visier genommen haben • Belege für Bedrohungen und Botnet-Aktivitäten, die gezielt die Kunden, Partner und Lieferanten eines Unternehmens ins Visier genommen haben • Branchenspezifische Analysen, einschließlich relevanter TTPs von Cyberkriminellen	• Stellen Sie die Verfügbarkeit und die korrekte Zuteilung der Ressourcen sicher, um die ermittelten Sicherheitslücken zu entschärfen • Due Diligence-Projekte über Dritte, um Angriffe auf die Lieferkette abzuwehren • Passen Sie Richtlinien und Kontrollen an, um potentielle Insider-Bedrohungen zu entschärfen • Steigern Sie das Sicherheitsbewusstsein Ihrer Mitarbeiter, indem Sie ein spezielles Programm basierend auf Ergebnissen entwickeln (z. B. durch externe Dienstleistungen gefährdete Anmeldedaten) • Verhindern Sie eine potenzielle Rufschädigung, indem Sie die unbefugte Verwendung von Unternehmensmarken zu Phishing-Zwecken überwachen • Planen und rechtfertigen Sie Investments in bestimmte Technologien, Mitarbeiter und Programme, die relevante Angriffsvektoren abdecken

Cyber Threats News: https://de.securelist.com/
IT Security News: https://www.kaspersky.de/blog/b2b/
IT-Sicherheit für KMUs: kaspersky.de/business
IT-Sicherheit für Großunternehmen: kaspersky.de/enterprise

www.kaspersky.de

Beständigkeit, Unabhängigkeit und Transparenz – das zeichnet uns aus. Wir möchten eine sicherere Welt schaffen, in der Technologien uns das Leben erleichtern. Deshalb schützen wir diese Technologien, damit Menschen auf der ganzen Welt die unzähligen Möglichkeiten nutzen können. Wir tragen mit Cybersicherheit zu einer sicheren Zukunft bei.

Erfahren Sie mehr unter kaspersky.de/transparency

Proven.
Transparent.
Independent.