VECTRA
SECURITY THAT THINKS

FORSCHUNGSBERICHT

Der Spotlight Report 2020 zu Office 365

INTELLIGENTE BEDROHUNGSERKENNUNG UND RESPONSE FÜR CLOUD-NATIVE UNTERNEHMEN

INHALTSVERZEICHNIS

Vectra® schützt Unternehmen durch Erkennen und Stoppen von Cyber-Angriffen

Als führender Anbieter für Netzwerk-Erkennung und Response (NDR) schützt Vectra Ihre Daten, Systeme und Infrastruktur. Mit Vectra kann Ihr Team Angriffsversuche erkennen und reagieren, noch bevor die Attacke startet.

Wir erkennen schnell verdächtige Verhaltensweisen und Aktivitäten in Ihrem gesamten lokalen und Cloud-Netzwerk, kennzeichnen sie und benachrichtigen Ihr Security-Team, damit es sofort reagieren kann.

Vectra steht für „Security that thinks®“. Mit künstlicher Intelligenz verbessern wir die Erkennung und Response im Laufe der Zeit und vermeiden False Positives – damit Sie sich auf die echten Bedrohungen konzentrieren können.

6,5–7 $ MILLIARDEN

Die Kosten durch Kontoübernahmen werden für mehrere Branchen auf 6,5–7 Milliarden US-Dollar pro Jahr geschätzt.

Forrester Wave: *Risk-Based Authentication* (Risikobasierte Authentifizierung), 3. Quartal 2017.

HIGHLIGHTS

4 Mio. **Microsoft Office 365-Konten wurden für diese Untersuchung analysiert**

96 % der untersuchten Kunden zeigten **laterale Bewegungen**

71 % der untersuchten Kunden zeigten **verdächtiges Verhalten von Office 365 Power Automate**

56 % der untersuchten Kunden zeigten **verdächtiges Verhalten von Office 365 eDiscovery**

Angreifer nutzen jede Gelegenheit und verursachen Chaos in der Cloud

Die Identität, und ganz konkret ihr Missbrauch und die Ausnutzung der darüber gewährten Zugriffsrechte, stellt in aktuellen SaaS-Umgebungen das größte Sicherheitsrisiko dar. Vor der Implementierung einer SaaS-Plattform müssen Sie sich zuerst Gedanken darüber machen, wie viele Zugriffsrechte einem Endanwender gewährt werden sollten.

Angreifer setzen inzwischen eher auf Kontoübernahmen als auf E-Mail-Kompromittierungen, um ins Unternehmensnetzwerk zu gelangen.

Noch wichtiger ist die Frage: Wofür werden diese Zugriffsrechte genutzt? Das Least-Privilege-Prinzip ist für SaaS-Umgebungen noch wichtiger, da hier nur die Identität kontrolliert wird und Daten sowie Ressourcen stark konsolidiert sind.

In der SaaS-Welt dominiert Office 365 mit mehr als 250 Millionen aktiven Nutzern pro Monat den Bereich der Produktivitätstools. Für viele dieser Anwender ist Office 365 das wichtigste Tool für Datenaustausch und -speicherung sowie Kommunikation – und wird damit zu einem äußerst lukrativen Ziel.

Wenig überraschend ist Office 365 daher ins Visier von Angreifern geraten. Trotz der zunehmenden Nutzung von MFA und anderen Sicherheitskontrollen nehmen die finanziellen und Rufschäden sowie Datenkompromittierungen in Office 365 immer weiter zu.

Bei den Ursachen für Datenlecks stehen Kontoübernahmen an erster Stelle. Angreifer setzen inzwischen eher auf Kontoübernahmen als auf E-Mail-Kompromittierungen, um einen Fuß in die Tür des Unternehmensnetzwerks zu bekommen.

Office 365-Konten werden heute missbraucht, um sich lateral zu anderen Anwendern mit umfassenderen Zugriffsrechten zu bewegen. Laut Daten von Vectra-Kunden zu 4 Millionen Konten für den Zeitraum von Juni bis August 2020 war Lateral Movement das am häufigsten beobachtete verdächtige Verhalten in Office 365-Umgebungen, dicht gefolgt von Command & Control-Kommunikation.

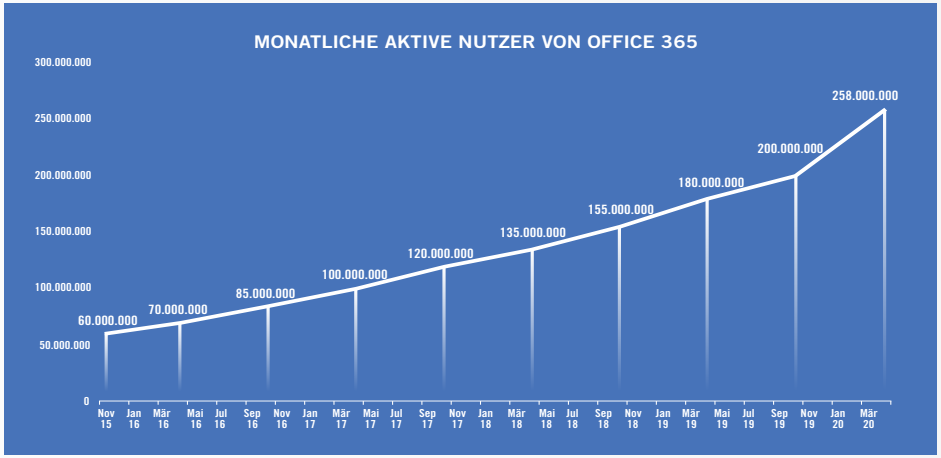


Abbildung 1: Monatliche aktive Nutzer von Office 365

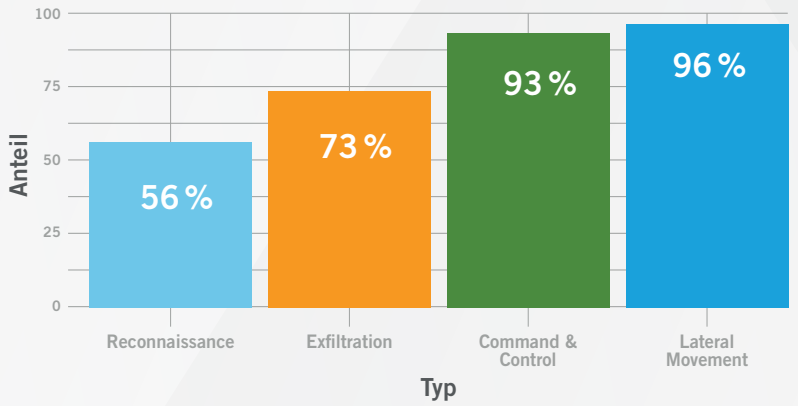


Abbildung 2: Häufigkeit der Kategorien verdächtiger Verhaltensweisen, die in Vectra NDR-Deployments mit Office 365 beobachtet wurden.

Die Cloud ist ein Einstiegspunkt und das Endziel von Angreifern, die sich auf der Suche nach lukrativen Daten lateral bewegen. In Office 365 durchlaufen die Bedrohungen den vollständigen Angriffsablauf, ohne dass ihre Aktivitäten auf Endgeräten oder im Netzwerk verzeichnet werden können, sodass herkömmliche Tools für Netzwerk- und Endgeräteerkennung unterlaufen werden.

Das bereitet heute große Probleme: Laut dem Forrester Wave-Bericht von 2017 zu risikobasierter Authentifizierung werden die Kosten durch Kontoübernahmen für mehrere Branchen auf 6,5–7 Milliarden US-Dollar pro Jahr geschätzt.

Von Office 365-Angreifern häufig eingesetzte Techniken

- Suche in E-Mails, Chatverläufen und Dateien nach Kennwörtern oder interessanten Daten
- Einrichtung von Weiterleitungsregeln, um permanent weitere E-Mails zu erhalten, ohne sich erneut anmelden zu müssen
- Nutzung eines vertrauenswürdigen Kommunikationskanals, um Mitarbeiter, Kunden und Partner anzugreifen (dabei fälscht der Angreifer die E-Mail-Adresse des CEO nicht nur, sondern nutzt sie tatsächlich)
- Einbindung von Malware oder schädlichen Links in Dokumenten, denen viele Menschen vertrauen und die häufig verwendet werden (auch hier wird Vertrauen missbraucht, um Präventionsmaßnahmen zu umgehen, die Warnungen auslösen könnten)
- Diebstahl oder Geiselnahme von Daten und Dateien

Das sind die offensichtlichen Angriffstechniken. Raffinierte Cyber-Kriminelle gehen jedoch mitunter deutlich geschickter vor.

LEGITIME TOOLS UND SERVICES, DIE VON OFFICE 365-ANGREIFERN MISSBRAUCHT WERDEN

Power Automate

Mit Microsoft Power Automate können Anwender eigene Integrationen und automatisierte Workflows zwischen Office 365-Anwendungen erstellen. Diese Funktion ist standardmäßig aktiviert und bietet Konnektoren für hunderte Drittanbieter-Anwendungen und -Services. Die allgemeine Verfügbarkeit und einfache Bedienung macht Power Automate zu einem nützlichen Tool für Angreifer, die böswillige Command & Control-Kommunikation und Lateral Movement koordinieren wollen.

eDiscovery

Microsoft eDiscovery ist ein elektronisches Erkennungstool, das Office 365-Anwendungen und -Daten durchsucht und die Ergebnisse exportiert. Angreifer nutzen eDiscovery als leistungsstarkes Tool für Internal Reconnaissance und die Exfiltration von Daten.

OAuth

OAuth ist ein offener Standard für die Authentifizierung von Zugriffen. Er wird von Drittanbieter-Anwendungen für die Authentifizierung der Endanwender mithilfe der Office 365-Anmeldedienste sowie der Anmeldedaten der Benutzer verwendet. Angreifer setzen auf böswillige Azure-Anwendungen mit OAuth-Funktionen, um persistenten Zugriff auf Office 365-Benutzerkonten zu gewährleisten.

Angreifer können Office 365 als Einstiegspunkt zum Benutzersystem und somit zu kontinuierlichen Zugriffen verwenden. Dazu können sie zum Beispiel E-Mail-Regeln einrichten, die durch Nachrichten mit einem bestimmten Betreff ausgelöst werden, oder sie synchronisieren einfach den Outlook-Client, um über das kompromittierte Office 365-Konto persistenten Reverse Shell-Zugriff auf das System des Anwenders zu erhalten.

Dabei sind zwei Office 365-Tools für Angreifer besonders nützlich: Power Automate und die eDiscovery-Compliance-Suche.

Diesen Wechsel von der Cloud zu den physischen Systemen nutzte die APT33-Gruppe (wahrscheinlich ein staatlich geförderter iranischer Akteur) für ihre Angriffe. APT33 erlangte per Password Spraying Zugriff auf Office 365 und erstellte anschließend E-Mail-Regeln, um auf den Systemen der kompromittierten Anwender ein Reverse Shell einzurichten.

Sobald APT33 in das physische Netzwerk gelangt war, folgte die Gruppe gängigen Angriffspfaden auf den physischen Systemen, um an Domain-Administratorrechte zu gelangen. Dieser Angriff zeigte, dass Cloud-basierte Systeme als Einstiegspunkte dienten und die physischen Systeme das eigentliche Ziel waren.

Angreifer sind auch geschickt darin, MFA für Office 365 zu umgehen, indem sie mit Social-Engineering-Techniken die Anwender zum Installieren böswilliger Azure-Anwendungen verleiten. Ebenso wie bei Mobilgeräte-Apps akzeptieren Anwender die Berechtigungsanfragen der Anwendungen, sodass die Angreifer ungehindert auf Ressourcen zugreifen können. Der Zugriff kann bis zu 90 Tage bestehen bleiben, ohne dass in der Zwischenzeit eine Authentifizierung verlangt wird – selbst wenn sich das Kennwort ändert.

Das größte Problem dabei: Angreifer nutzen jede Gelegenheit und missbrauchen legitime Office 365-Tools und -Funktionen, um sich vor Sicherheitskontrollen zu verbergen bzw. diese zu umgehen.

Angriffe mit dieser Taktik richteten sich gegen Unternehmen in Australien und wurden häufig Akteuren in China zugeordnet. Bei diesem Social-Engineering-Trick wurde eine Version der Sicherheitsanwendung MailGuard 365 gefälscht, die von den angegriffenen Unternehmen bereits genutzt wurde. Nach der Installation erhielten die Angreifer persistenten Zugriff und konnten Benutzerprofile lesen sowie E-Mails manipulieren.

Das größte Problem dabei: Angreifer nutzen jede Gelegenheit und missbrauchen legitime Office 365-Tools und -Funktionen, um sich vor Sicherheitskontrollen zu verbergen bzw. diese zu umgehen. Dabei sind zwei Office 365-Tools für Angreifer besonders nützlich: Power Automate und die eDiscovery-Compliance-Suche.

Microsoft Power Automate (früher Microsoft Flow) automatisiert alltägliche Aufgaben wie die Verwaltung von E-Mail-Anhängen oder Genehmigungsflows. Diese Funktion wird für alle Office 365-Kunden standardmäßig aktiviert und kann so konfiguriert werden, dass Anwender – oder eben auch Angreifer – erheblichen Zeit- und Arbeitsaufwand sparen. Dazu gehören:

- Herstellen einer HTTP-Verbindung zu einem Command & Control-Punkt zum Versenden von Daten
- Automatische Synchronisation von OneDrive-Dateien bei jeder Dateiänderung mit einem Google Drive-Konto, das dem Angreifer gehört
- Tweeten aller E-Mails, die bestimmte Schlüsselwörter enthalten

Dank mehr als 350 Konnektoren für Anwendungen (wobei jede Woche neue hinzukommen) bietet Power Automate den Cyber-Angreifern unzählige Möglichkeiten.

Die Compliance-Suche von Office 365 eDiscovery bietet eine zentrale Suchfunktion für alle Office 365-Anwendungen. So können zum Beispiel mit einem einfachen Befehl Microsoft Outlook, Teams, alle Dateien in SharePoint und OneDrive sowie OneNote-Notizbücher nach „Kennwort“ oder „Passwort“ durchsucht werden.

Alle diese Techniken werden heute aktiv und häufig auch gemeinsam für den gesamten Angriffsablauf eingesetzt. Power Automate und eDiscovery gehören zu den häufigsten verdächtigen Verhaltensweisen in Office 365-Umgebungen von Vectra-Kunden.

Zur Unterstreichung der Risiken durch native Office 365-Tools veröffentlichte Microsoft die Zeitleiste eines Angriffs, der mit standardmäßigen Techniken für 240 Tage vollständigen Office 365-Zugriff ermöglichte. Dabei nutzten die Angreifer eDiscovery zur Suche nach Daten und anschließend Power Automate, um sie zu exfiltrieren.

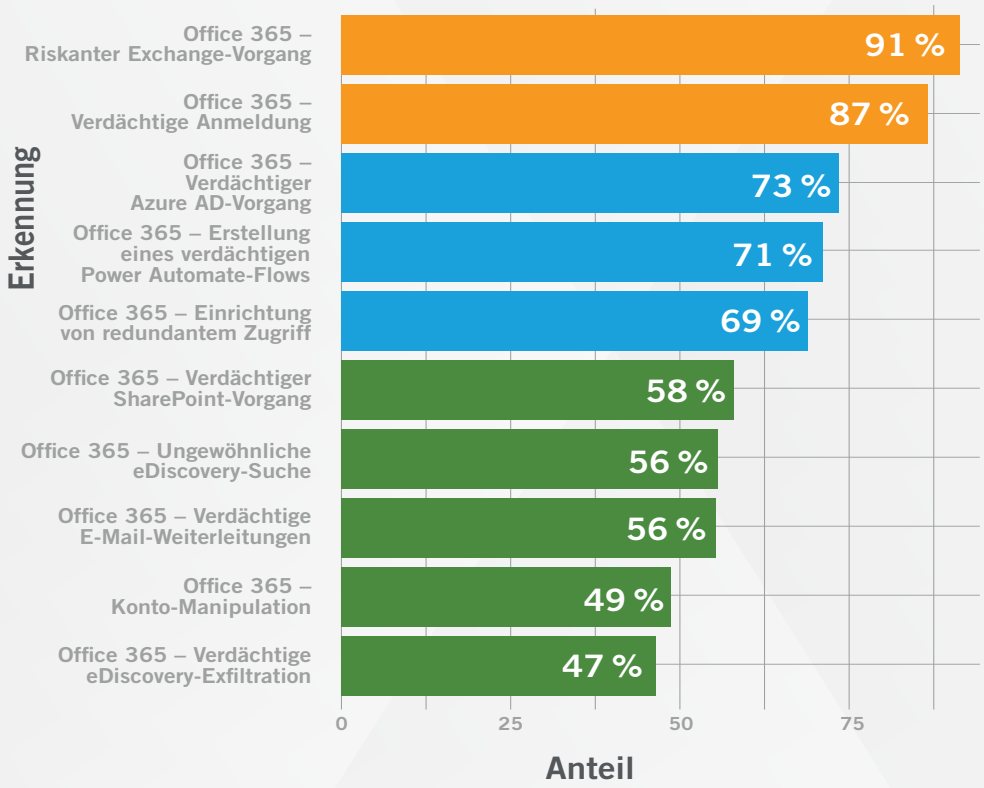


Abbildung 3: Häufigkeit der Top 10 der verdächtigen Verhaltensweisen, die in Vectra NDR-Deployments mit Office 365 beobachtet wurden.

Eine Analyse von 4 Millionen Office 365-Konten, die von Vectra überwacht wurden, ergab eine Liste der zehn häufigsten Verhaltensweisen, die mit Angriffen auf Office 365 in Verbindung gebracht wurden. Diese Verhaltensweisen bezogen sich vor allem auf Bedrohungsakteure, die Angriffstechniken mit Command & Control und Lateral Movement einsetzten.

MITRE ATT&CK-Zuordnung: Top 10 der verdächtigen Verhaltensweisen, die in Vectra NDR-Deployments mit Office 365 beobachtet wurden

MITRE ATT&CK™

Vectra-Erkennung in Office 365	MITRE ATT&CK-Framework	Zugeordnetes Angreiferverhalten
Riskanter Exchange-Vorgang	• T1484 – Änderung der Gruppenrichtlinie • T1098 – Konto-Manipulation	**Lateral Movement** Ein Angreifer manipuliert Microsoft Exchange, um auf einen bestimmten Datensatz zuzugreifen oder dafür zu sorgen, dass der Angriff fortgesetzt werden kann.
Verdächtige Anmeldung	• T1078 – Gültige Konten	**Command & Control** Ein Angreifer hat die Zugangsdaten für ein gültiges Konto gestohlen und verwendet sie für einen Angriff.
Verdächtiger Azure AD-Vorgang	• T1078 – Gültige Konten	**Lateral Movement** Ein Angreifer erweitert Berechtigungen und führt Prozesse mit Administratorrechten aus, nachdem er ein Standortkonto übernommen hat.
Erstellung eines verdächtigen Power Automate-Flows	• T1041 – Exfiltration über C&C-Kanal • T1008 – Fallback-Kanäle • T1105 – Eingehende Tool-Übertragung • T1059 – Befehls- und Skript-Interpreter • T1020 – Automatisierte Exfiltration	**Command & Control** Ein Angreifer nutzt Power Automate als Persistenz-Mechanismus innerhalb der Umgebung.
Einrichtung von redundantem Zugriff	• T1098 – Konto-Manipulation	**Command & Control** Ein Angreifer nutzt den Zugriff auf eine sensible Rolle, um redundanten Zugriff auf das Netzwerk zu ermöglichen.
Verdächtiger SharePoint-Vorgang	• T1078 – Gültige Konten • T1213 – Daten aus Informations-Repositorys	**Lateral Movement** Ein Angreifer hat ein SharePoint-Administratorkonto gefunden und verwendet es für die Fortsetzung des Angriffs.
Ungewöhnliche eDiscovery-Suche	• T1119 – Automatisierte Erfassung • T1213 – Daten aus Informations-Repositorys • T1083 – Suche nach Dateien und Verzeichnissen	**Internal Reconnaissance** Ein Angreifer kann auf eDiscovery-Funktionen zugreifen und verwendet sie für Internal Reconnaissance innerhalb der Umgebung.
Verdächtige E-Mail-Weiterleitungen	• T1114 – E-Mail-Erfassung	**Exfiltration von Daten** Ein Angreifer hat persistenten Zugriff auf die Inhalte eines bestimmten Postfachs erhalten, ohne dazu eine Software installieren zu müssen.
Konto-Manipulation	• T1098 – Konto-Manipulation	**Lateral Movement** Ein Angreifer hat die Zugriffsrechte für ein Microsoft Exchange-Konto erweitert, um BEC zu ermöglichen oder weitere Informationen für die nächste Angriffsphase zu sammeln.
Exfiltration über eDiscovery	• T1048 – Exfiltration über alternatives Protokoll	**Exfiltration von Daten** Ein Angreifer kann auf eDiscovery-Funktionen zugreifen und verwendet sie zum Erfassen oder Exfiltrieren von Daten.

Kundenbeispiel: Mittelständischer Hersteller

Hersteller per Business-Email Compromise (BEC) angegriffen

Der Angreifer informierte sich über die Finanzabteilung, wahrscheinlich über LinkedIn. Dann startete er einen langsamen, unauffälligen Brute-Sweep-Angriff auf ältere Protokolle (auch hier ein Bereich, in dem MFA nicht umsetzbar ist), um Zugriff auf Office 365 zu erlangen.

Sobald der Angreifer einen Fuß in der Tür hatte, richtete er Regeln ein, damit alle E-Mails mit DocuSign- oder Rechnungsbezug weitergeleitet wurden. Das zeigte deutlich das Interesse an Finanzbetrug. Clevererweise erstellte der Angreifer eine weitere Regel, die alle Hinweise auf die Bedrohung sowie alle E-Mails zu Kennwörtern und Sicherheitsfragen automatisch löschte.

Vectra erkannte in Echtzeit mehrere Phasen des Angriffs und ermöglichte es dem Security-Team, die Weiterleitungsregeln zu löschen und die Kennwörter zu ändern, bevor auch nur eine E-Mail nach außen gelangte.

Erkennungen

Brute-Force-Angriff → **Verdächtige Anmeldung** → **Riskanter Exchange-Vorgang** → **Verdächtige E-Mail-Weiterleitungen**

Mehrere erfolglose Versuche, gefolgt von einem erfolgreichen. Die IP-Adresse war für das Konto ungewöhnlich.

Die Anmeldung erfolgte über einen lokalen Proxy. Der Benutzer-Agent und die Authentifizierungsmethode waren für das Konto jedoch ungewöhnlich.

Es wurden riskante Postfach-Verwaltungsaktionen durchgeführt, die zulässig, aber ungewöhnlich waren.

Es wurden Weiterleitungsregeln an eine externe Adresse erstellt, die für das Konto ungewöhnlich waren.

Abbildung 5: Vectra-Erkennungen bei einem BEC-Versuch.

Kundenbeispiel: Forschungsuniversität

Die medizinische Forschungsabteilung einer Universität wurde mit einem Phishing-Köder angegriffen, der für eine kostenlose Anwendung für Kalenderoptimierung und Zeitmanagement warb.

Eine Person biss an und installierte die böswillige OAuth-Anwendung, die die MFA-Vorgaben umging und unbemerkt vollständigen Zugriff auf Office 365 gewährte.

Über diese Anwendung konnten die Angreifer interne Phishing-E-Mails versenden und die vertrauenswürdigen Identitäten und Kommunikationskanäle nutzen, um sich in der Universität weiter zu verbreiten.

Vectra erkannte die Installation der verdächtigen Anwendung und stellte bei der Untersuchung das interne Spearphishing fest. Das Security-Team konnte den Angreifer durch die Entfernung der böswilligen Anwendung erfolgreich blockieren.

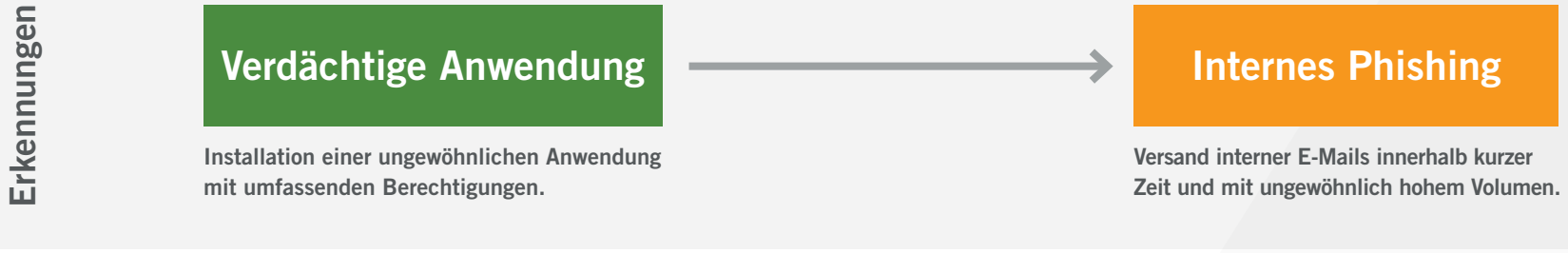
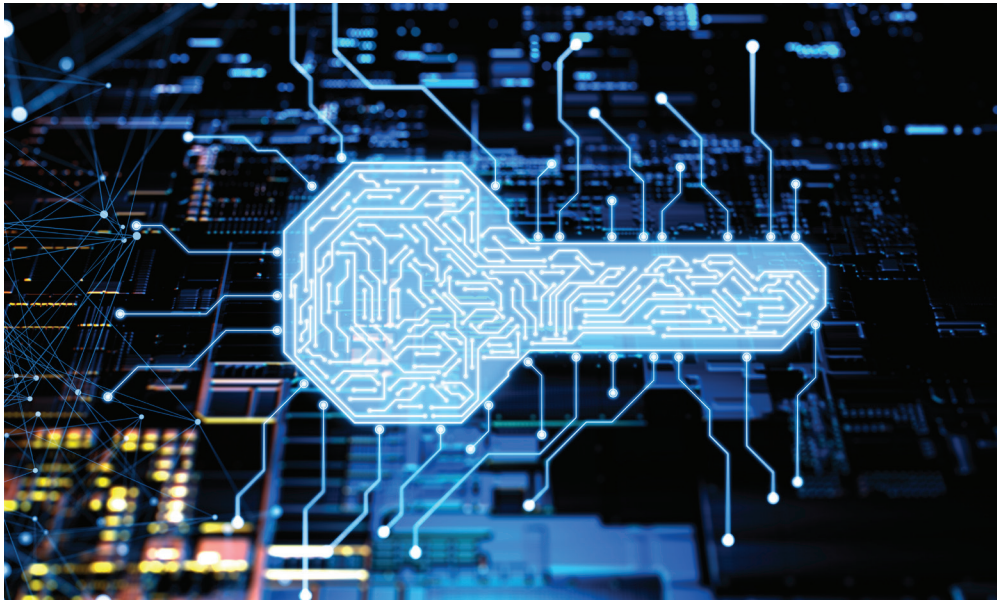


Abbildung 6: Vectra-Erkennung von Angriffen mit MFA-Umgehung.

Schutz Ihrer Office 365-Deployments

Die Erkennung des Missbrauchs von Anwenderzugriffen wurde bislang als statisches Problem betrachtet. Dabei wurden präventions- und richtlinienbasierte Ansätze oder manuelle Berechtigungen eingesetzt, die auftretende Bedrohungen sichtbar machen und wenig Zeit für eine angemessene Response bieten. Diese veralteten Ansätze sind wirkungslos geworden.

Eine solche Zugriffsüberwachung zeigt lediglich, dass ein genehmigtes Konto für den Zugriff auf Ressourcen verwendet wird, bietet dabei aber keinen Einblick darin, wie und warum diese Ressourcen genutzt werden.



Es genügt nicht, sich lediglich auf die gewährten Rechte einer Entität zu konzentrieren oder die Rechte komplett außen vor zu lassen. Security-Teams benötigen detaillierten Kontext, der ihnen zeigt, wie Entitäten ihre Rechte (das beobachtete Recht) in SaaS-Anwendungen wie Office 365 verwenden. Angreifer beobachten oder unterbinden Interaktionen zwischen Entitäten – die Verteidiger sollten in Bezug auf die Kriminellen ebenso vorgehen.

Dadurch verstehen die Security-Teams, wie und von wo Anwender auf Office 365-Ressourcen zugreifen, allerdings ohne die vollständigen Nutzdaten anzusehen. Dadurch wird die Privatsphäre geschützt. Relevant sind hier Nutzungsmuster und Verhaltensweisen, nicht der statische Zugriff.

Angesichts der großen Anzahl von Angriffen kann nicht genug betont werden, welchen Stellenwert der Missbrauch von Anwenderzugriffen haben muss. In SaaS-Plattformen wie Office 365 können sich Angreifer ungehindert lateral bewegen. Daher ist es wichtig, sich auf die Zugriffe der Anwender auf Konten und Services zu konzentrieren.

Wenn Security-Teams zuverlässige Informationen und realistische Erwartungen zu SaaS-Plattformen haben, sollte es ihnen deutlich leichter fallen, böswilliges Verhalten und Rechtemissbrauch schnell zu erkennen und zu beheben.

Security-Teams benötigen detaillierten Kontext, der ihnen zeigt, wie Entitäten ihre Rechte (das beobachtete Recht) in SaaS-Anwendungen wie Office 365 verwenden.

E-Mail: info_dach@vectra.ai vectra.ai/de