Darktrace Cyber-KI: Kompromittierung von E-Mail-Zugangsdaten

Unternehmen werden sich erst dann bewusst, wie wertvoll ein E-Mail-Postfach ist, wenn es in die falschen Hände gelangt. Sind die Bedrohungsakteure erst einmal eingedrungen, bieten sich ihnen jede Menge Angriffsmöglichkeiten. Es ist alarmierend, wie einfach sich Angreifer Zugriff verschaffen können, sei es durch Phishing-Kampagnen, Brute-Force-Angriffe oder Austausch im Dark Web.

In vielen Fällen stehlen die Angreifer Posteingänge, weil sie es auf die darin enthaltenen wertvollen Daten abgesehen haben. Persönliche Informationen aus privaten Chats oder sensible Abrechnungsdaten können für Betrug oder Erpressung missbraucht werden, während aus alten E-Mail-Threads streng vertrauliche Unternehmensinformationen herausgefiltert werden können. Kundenlisten, Preislisten oder Informationen zu Roadmaps und geistigem Eigentum sind meist schnell gefunden.

In anderen Fällen nutzen Cyberkriminelle das Konto als Startrampe für die nächsten Phasen eines Angriffs. Sie lauern im Verborgenen und sammeln seelenruhig Informationen über Führungskräfte oder Partner, die für sie von hohem Nutzen sind – dazu lesen sie Dokumente, verfolgen Korrespondenz und finden heraus, wie sie unbemerkt zuschlagen können. Wie bei der Kaperung von Supply-Chain-Konten ist die Fähigkeit, den E-Mail-Verkehr zu verfolgen und mit einer plausiblen Antwort anzugreifen, häufig der effizienteste Weg, einen Angriff zu starten, ohne dass Verdacht geschöpft wird.

Abbildung 1: Darktrace Threat Visualizer zeigt geografische Anmeldeorte an

Unternehmensweiter Kontext

Die Möglichkeiten für die Angreifer sind nahezu unendlich, für die Verteidiger hingegen sind sie begrenzt. Einfache und statische Sicherheitsmechanismen (einschließlich „Impossible Travel"-Regeln) überwachen zwar Unternehmenskonten, damit diese nicht gekapert werden. Gewiefte Angreifer jedoch, die genau wissen, wie sie in das Unternehmen eindringen können, lassen sich dadurch nicht abhalten. Das Enterprise Immune System von Darktrace gleicht die Schwächen regelbasierter Ansätze aus und fängt diejenigen Cyber-Bedrohungen ab, die die Verteidigungslinie passieren.

So wie das menschliche Immunsystem nutzt auch die Cyber-KI von Darktrace das tiefgehende Wissen über die normale Funktionsweise des eigenen „Ichs", um schädliches Verhalten zu erkennen, das sonst unbemerkt bliebe. Darktrace macht sich ein Bild von den normalen Verhaltensmustern, den sogenannten „Patterns of Life", jedes Benutzers und Geräts im Unternehmen und erkennt dadurch subtile Abweichungen, die selbst den vorsichtigsten Angreifer verraten – ganz gleich, ob diese Abweichungen sich in verdächtigem Anmeldeverhalten, der Erstellung von Posteingangsregeln oder Änderungen der Benutzerrechte manifestieren. Da Cyberbedrohungen immer ausgefeilter werden, ist selbstlernende KI der einzig wirksame Weg, um Posteingänge vor Kriminellen zu schützen.

Fallstudie 1: Automatisierter Brute-Force-Angriff

Bei einem anderen Unternehmen stellte Darktrace täglich über einen Zeitraum von einer Woche mehrere fehlgeschlagene Anmeldeversuche bei einem Microsoft 365-Konto immer mit denselben Benutzernamen fest. Jede Anmelderunde erfolgte an sechs Tagen immer genau um 18.04 Uhr. Dass Uhrzeit und Anzahl der Anmeldeversuche an jedem Tag immer gleich waren, deutete auf einen automatisierten Brute-Force-Angriff hin, der so programmiert war, dass nach einer bestimmten Anzahl an Fehlversuchen Schluss war, um eine Kontosperrung zu vermeiden.

Darktrace stufte dieses Muster als äußerst anormal ein und benachrichtigte das Sicherheitsteam. Hätte Darktrace nicht die schwachen Indikatoren in Beziehung gesetzt und die subtilen Hinweise auf die sich entwickelnde Bedrohung erkannt, hätte dieser automatisierte Angriff noch Wochen oder Monate andauern können und der Angreifer hätte anhand anderer bereits gesammelter Informationen die Kennwörter der Benutzer erraten können.

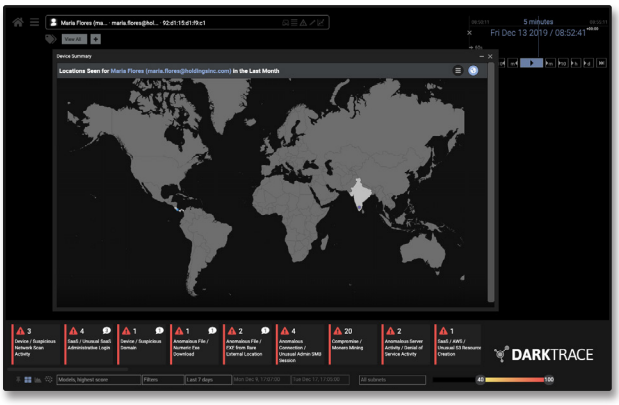

Abbildung 2: Schaubild zur Veranschaulichung der wiederholten Anmeldeversuche

03/12 20:45:39	Saas::Admin	Regular	UpdateUser
03/12 20:45:39	Saas::Admin	Regular	ChangeUserLicense
03/12 20:26:43	Saas::Login	Regular	UserLoggedIn
03/12 20:26:43	Saas::FailedLogin	Regular	UserLoginFailed
03/12 20:26:36	Saas::FailedLogin	Regular	UserLoginFailed
03/12 18:31:31	Saas::Login	Regular	UserLoggedIn
03/12 17:57:46	Saas::Admin	Regular	ChangeUserLicense
03/12 17:57:46	Saas::Admin	Regular	UpdateUser
03/12 17:06:57	Saas::Admin	Regular	UpdateUser

Abbildung 3: Die mit dem SaaS-Konto verbundene Aktivität, Änderung der Zugangsdaten wurde hervorgehoben

Fallstudie 2: Kompromittierung und Sabotage eines Microsoft 365-Kontos

Bei einer internationalen Non-Profit-Organisation mit Büros in aller Welt erkannte Darktrace, dass in Microsoft 365 ein Konto gekapert worden war, weil die statische „Impossible Travel"-Regel von Azure AD den Angriff nicht abgewehrt hatte. Die selbstlernende KI von Darktrace erkannte einen Anmeldevorgang von einer IP-Adresse aus, die ungewöhnlich für die betreffende Benutzerin und ihre Peer-Group war, und benachrichtigte sofort das Sicherheitsteam.

Darktrace wies darauf hin, dass für das Konto eine neue E-Mail-Verarbeitungsregel eingerichtet wurde, die eingehende und ausgehende E-Mails löscht. Dies war ein deutlicher Hinweis auf eine Kompromittierung und das Sicherheitsteam konnte das Konto sperren, bevor der Angreifer Schaden anrichten konnte.

Mit dieser neuen E-Mail-Verarbeitungsregel hätte der Angreifer E-Mail-Korrespondenz mit anderen Mitarbeitern im Unternehmen führen können, ohne dass der legitime Benutzer etwas davon mitbekommen hätte. Dies ist eine beliebte Strategie von Cyberkriminellen, um sich dauerhaften Zugriff zu verschaffen und sich im Unternehmen einzunisten, möglicherweise als Vorbereitung für einen großangelegten Angriff.

Durch Analyse der ungewöhnlichen IP-Adresse in Verbindung mit dem unüblichen Verhalten des scheinbaren Benutzers identifizierte Darktrace diese Aktivität als Kontoübernahme und verhinderte damit größeren Schaden für das Unternehmen.

Abbildung 4: Veranschaulichung der wiederholten Anmeldeversuche