P R E S S E M I T T E I L U N G

Delinea Produkt-Update: Neues Workstation-Policy-Framework kann Schäden durch Phishing reduzieren

Sofort einsatzbereite Richtlinien schützen Kunden vor den gängigsten Angriffen auf privilegierte Workstation-Zugriffe

München, 27. Juni 2023 – **Mit der neuesten Version des bewährten Privilege Managers von Delinea, dem Spezialisten für Lösungen, die Privileged-Access Management (PAM) nahtlos erweitern, lassen sich Benutzer- und Anwendungsberechtigungen auf Workstations fortan noch benutzerfreundlicher kontrollieren. So können fünf der gängigsten Richtlinien zur Erhöhung der Berechtigungen von nun an über das neue Workstation-Policy-Framework vorkonfiguriert werden, um die Implementierung zu vereinfachen und den Zeitaufwand zu verkürzen.**

Laut dem Verizon Data Breach Investigations Report 2023 lassen sich 44 Prozent aller Social-Engineering-Vorfälle auf Phishing zurückführen. Trotz steigender Aufklärung klicken 84 Prozent der Mitarbeitenden innerhalb der ersten 10 Minuten nach Erhalt einer Phishing-E-Mail auf einen manipulierten Link oder bösartige Attachments oder antworten mit sensiblen Informationen. Zudem werden 70 Prozent der mit Malware infizierten Dateianhänge und Links nicht von Netzwerksicherheitslösungen geblockt, wie die U.S. Cybersecurity & Infrastructure Security Agency zeigt. Für Angreifer ist es dann ein Leichtes, den Endpunkt zu kompromittieren, Berechtigungen zu erhöhen und sich lateral im Netzwerk zu bewegen, um sensible Daten aufzuspüren und zu exfiltrieren.

Ohne eine angemessene Kontrolle von privilegierten Zugriffen auf Workstations sind Unternehmen anfällig für Phishing, selbst wenn andere Sicherheitslösungen im Einsatz sind. Konkret bedeutet dies, dass für Benutzer und Anwendungen spezielle Richtlinien zur Erhöhung der Zugriffsrechte festgelegt werden müssen, um einen besseren Schutz vor Malware und Phishing-Betrug zu gewährleisten.

Vereinfachte Richtlinien für den privilegierten Zugriff auf Workstations bedeuten mehr Sicherheit und weniger Reibungsverluste

Privilege Manager setzt Just-Enough-Berechtigungen durch, die genehmigte Geschäftsaktivitäten unterstützen, und blockiert oder beschränkt gleichzeitig Berechtigungen, die von Malware ausgenutzt werden könnten. Dieser Ansatz reduziert die Reibungsverluste und steigert die Produktivität bei gleichzeitiger Optimierung der Sicherheit.

Das neue Workstation Policy Framework basiert auf Delineas jahrelanger Erfahrung sowie dem Kundenfeedback. Es umfasst fünf der gängigsten Richtlinien, die Kunden dabei unterstützen, sichere Zugriffe auf Windows- und Mac-Workstations zu gewährleisten, ohne die Produktivität der Benutzer zu beeinträchtigen. Bestehende Kunden können ihre Richtlinien mit dem neuen Framework vergleichen und die Richtlinien einführen, die in ihren Umgebungen möglicherweise noch fehlen.

Zu den fünf vorkonfigurierten Richtlinien gehören:

1. **Malware Attack Protection:** Diese Richtlinie verhindert, dass LOLBAS (Living Off the Land Binaries and Scripts)-Angriffe von häufig ausgenutzten übergeordneten Anwendungen ausgeführt werden. LOLBAS ist eine Angriffsmethode, bei der bereits vorhandene Tools und ausführbare Dateien missbraucht werden, die Teil des Betriebssystems sind.

2. **Allow Microsoft Signed Security Catalog:** Diese Richtlinie erlaubt die Ausführung von Microsoft-signierten Sicherheitskatalog-Installationsprogrammen. Sie kann mit Blocklisten-Richtlinien kombiniert werden, um zu verhindern, dass legitime Betriebssystemanwendungen blockiert werden.

3. **Software Development Tools:** Diese Richtlinie zielt auf gängige Systemprozesse für Softwareentwicklungslösungen ab, einschließlich untergeordneter Prozesse, und minimiert Verzögerungen, die durch die Anforderung von Berechtigungserhöhungen entstehen.

4. **Visual Studio Installers:** Mit dieser Richtlinie werden vier definierte Microsoft Visual Studio-Installationsprogramme vorab genehmigt und stillschweigend erhöht.

5. **Capture Application Elevation Attempts:** Diese Richtlinie zielt auf Nicht-Microsoft-Anwendungen ab, die eine UAC-Eingabeaufforderung auslösen, und sendet Richtlinien-Feedback, um Richtlinienanpassungen zu bewerten, die Anwendungen zulassen, erhöhen oder blockieren können.

Positive Auswirkungen auf Entwickler und IT-Verwaltungstools

Dank einer weiteren wesentlichen Verbesserung dieser Version kann eine granulare Kontrolle über das Hinzufügen, Ändern oder Löschen von Benutzern auf Workstations über PowerShell umgesetzt werden – selbst in PowerShell-Sitzungen mit vollständig erweiterten Berechtigungen. Dies verringert das Risiko, dass Entwickler und IT-Administratoren die PowerShell-Funktionen missbrauchen, und kann die Auswirkungen von bösartigem Code und Ransomware reduzieren. Eine solche granulare Steuerung von Hinzufügungs-, Änderungs- und Löschvorgängen verringert zudem das Risiko von Lateralbewegungen durch einen bösartigen Akteur erheblich.

„Sicherheitslösungen bedeuten nur dann einen Mehrwert, wenn sie benutzerfreundlich sind und die Produktivität des Unternehmens nicht beeinträchtigen“, so Dmitriy Ayrapetov, Vice President of Product Management bei Delinea. „Unsere Mission ist es, Sicherheit nahtlos zu gestalten. Diese Version des Privilege Managers berücksichtigt das Feedback unserer Kunden und ermöglicht es den Anwendern, von einer einfacheren Richtlinienverwaltung, besserer Sicherheit und weniger Reibungsverlusten zu profitieren und so wertvolle Zeit bei der Verwaltung unserer Lösung zu sparen.“

Weitere Aktualisierungen in dieser Version umfassen mehr Flexibilität bei der Steuerung von Firewall-Einstellungen sowie Verbesserungen an der Benutzeroberfläche hinsichtlich der Zugänglichkeit.

Eine kostenlose Testversion der neuesten Version von Privilege Manager kann hier angefordert werden: https://delinea.com/de/products/privilege-manager

Über Delinea
Delinea ist ein führender Anbieter von Privileged-Access-Management (PAM)-Lösungen für moderne, hybride Unternehmen. Die Delinea Platform erweitert PAM nahtlos, indem sie eine identitätsübergreifende Autorisierung bereitstellt und den Zugriff auf die kritischsten Hybrid-Cloud-Infrastrukturen sowie die sensibelsten Daten eines

Unternehmens kontrolliert. Auf diese Weise werden Risiken reduziert, Compliance gewährleistet und die Sicherheit vereinfacht. Die Kundenbasis von Delinea umfasst Tausende Unternehmen weltweit und reicht von KMUs bis hin zu den weltweit größten Finanzinstituten und Unternehmen der kritischen Infrastruktur. Weitere Infos unter: http://delinea.com/de

Erfahren Sie mehr über Delinea auf LinkedIn, Twitter und YouTube.

Pressekontakte:

Delinea DACH
Claudia Specht, Senior Marketing Manager DACH
claudia.specht@delinea.com

PR-Agentur: Weissenbach PR
Dorothea Keck
T: +49 89 54 55 82 02
delinea@weissenbach-pr.de
Web: www.weissenbach-pr.de