Auszug aus dem H&G Kundenmagazin Read:IT

Die vollständige Ausgabe finden Sie unter: www.hug.de/readit-magazin/

Endpoint-Security

WENN DER ANHANG KEINE RECHNUNG, SONDERN MALWARE WAR …

Ein unbedachter Klick auf E-Mail-Anhänge oder Datei-Downloads kann Auslöser für schwerwiegende Cyberangriffe sein. HP Sure Click Enterprise setzt auf Threat Isolation anstatt nur Threat Detection: Die Lösung isoliert Dateien und Websites, damit selbst unbekannte Angriffsmethoden wirkungslos verpuffen.

Wenn Fachkräfte rar sind, wird jede Bewerbung in der Personalabteilung begeistert aufgenommen – und das angehängte PDF geöffnet. Firewall und Antivirenscanner sorgen dafür, dass als Bewerbung getarnte Angriffe von Hackern erfolglos bleiben. Aber was passiert bei unbekanntem Schadcode oder neuen Angriffsvektoren, die Firewall und Antivirensoftware unterlaufen? Die Malware breitet sich im Unternehmensnetzwerk aus und öffnet dem Angreifer Tür und Tor. Für das IT-Personal beginnt ein Wettlauf gegen die Zeit.

Cyberkriminelle gehen geschickt vor. Sie versenden täuschend echte E-Mails mit versteckter Malware im Anhang oder erschleichen sich das Vertrauen von Mitarbeitenden in sozialen Medien, um ihnen Dateien oder Phishing-Links unterzuschieben. Entsprechend groß ist die Verunsicherung: Ein unbedachter Klick kann eine Organisation Millionenbeträge kosten und die Reputation beinträchtigen. Gängige Sicherheitslösungen, die nach dem Prinzip der Bedrohungserkennung (Threat Detection) arbeiten, reichen nicht aus. Immer wieder gelingt es Hackern, etablierte Abwehrmechanismen zu überwinden. HP Sure Click Enterprise ergänzt diese daher um eine zusätzliche Schutzschicht, die sowohl Anwender als auch IT-Administratoren im Alltag entlastet.

HP Sure Click Enterprise nimmt alle Bedrohungen in Isolationshaft

Unabhängig davon, woher die Datei stammt, öffnet HP Sure Click Enterprise E-Mail-Anhänge, Office-Dokumente, Browser-Tabs, Dateien in so genannten Micro-Virtual-Machines (Micro-VM). Im Gegensatz zu herkömmlichen virtuellen Maschinen, die eine vollständige Betriebssysteminstanz enthalten, sind Micro-VMs darauf ausgelegt, Anwendungen oder Prozesse in einer isolierten Umgebung mit geringem Ressourcenbedarf auszuführen. Dies funktioniert mit HP Sure Click Enterprise auf allen Rechnern, auf denen Windows läuft und die prinzipiell VMs erstellen können.

Jede Micro-VM verfügt über eigene Ressourcen wie Speicher, CPU-Zyklen sowie Netzwerkschnittstellen und funktioniert als eine vom Rest des Systems abgeschnittene Umgebung. Diese Isolierung reduziert die Angriffsfläche: Bösartiger Code kann nicht auf andere Anwendungen oder das Betriebssystem übergreifen. Schließt der Benutzer die Datei oder den Browser-Tab, wird die Micro-VM zerstört und damit die darin enthaltene Bedrohung.

Trotz Malware können Anwender einfach weiterarbeiten

Antivirenlösungen arbeiten nach dem Prinzip der Angriffserkennung (Threat Detection) – sie suchen nach den typischen Signaturen und Verhaltensmustern von Malware, um sie zu identifizieren und unschädlich zu machen. Dieses Prinzip funktioniert bei bekannten Bedrohungen in der Regel zuverlässig, stößt aber bei unbekanntem Code an seine Grenzen. Bei HP Sure Click Enterprise spielt die Signatur der Malware keine Rolle, da alles, was potentiell schädlichen Code enthalten könnte, abgeschottet wird. Der Benutzer kann ohne Bedenken Anhänge und Dateien öffnen, unabhängig von ihrer Herkunft.

Für die Anwender entstehen im Alltag keine Einschränkungen. Erhalten sie etwa ein Office-Dokument, müssen sie sich keine Gedanken darüber machen, ob darin eine Malware versteckt sein könnte. Es spielt auch keine Rolle, woher die Datei stammt – nur der Dateityp ist entscheidend. Anwender können das Dokument öffnen, bearbeiten und sogar Daten aus der Zwischenablage einfügen. Alle Änderungen bleiben erhalten, auch wenn die Micro-VM geschlossen und gelöscht wird. Öffnen die Anwender die Datei erneut, geschieht dies in einer neuen, nicht recycelten Micro-VM. Das gilt auch, wenn das Dokument innerhalb des Unternehmens weitergeleitet wird.

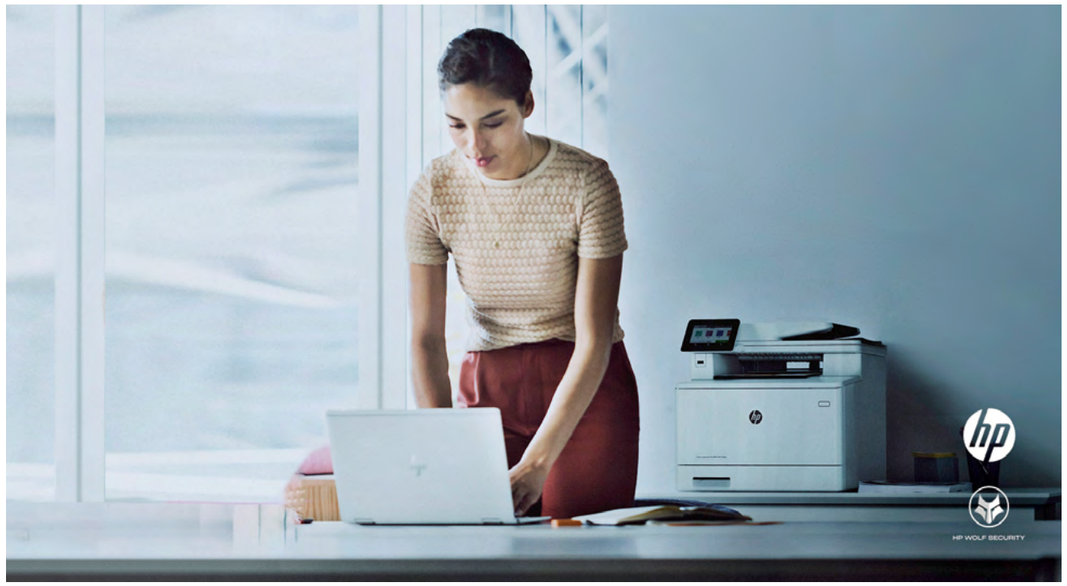
Flexible Anpassung durch Gruppenrichtlinien

Da in den meisten Unternehmen bestimmte Bereiche besonders geschützt werden müssen, während andere Benutzer mehr Flexibilität benötigen, bietet HP Sure Click Enterprise eine richtlinienbasierte Zugriffssteuerung. Administratoren können den sicheren Web- und Dateizugriff für Benutzergruppen konfigurieren und fein abgestufte Standardrichtlinien für häufige Anwendungsfälle wie E-Mail-Anhänge, Office-Dokumente, PDF-Dateien und Downloads aus dem Internet definieren. Ein Administrator kann beispielsweise festlegen, dass eine bestimmte Benutzergruppe Dateien als vertrauenswürdig markieren und den Schutz aufheben darf.

Die Verwendung einer Micro-VM kann auch von bestimmten Faktoren abhängig gemacht werden, wie zum Beispiel dem E-Mail-Server, von dem eine Datei stammt, oder von der verwendeten Anwendung und ob eine Benutzergruppe über VPN auf das Unternehmensnetzwerk zugreift oder nicht. Es ist auch möglich, Websites temporär freizuschalten, so dass Mitarbeitende diese für eine Sitzung ohne Micro-VM öffnen können.

BSI EMPFIEHLT DIE TECHNOLOGIE HINTER HP SURE CLICK ENTERPRISE

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bewertet den Nutzen der Isolationstechnologien mit Hilfe von Micro-VMs in dem 2022 erschienenen Maßnahmenkatalog Ransomware als „sehr gut“.



Die Abfrage von Zugangsdaten wird blockiert

Eine weitere Stärke der Lösung ist der Schutz vor Websites, die von Kriminellen für Phishing-Angriffe verwendet werden. Cyberkriminelle versuchen immer wieder, Anwender über Phishing-Links auf seriös aussehende, aber gefälschte Websites zu locken, um Zugangsdaten abzufragen. Wenn Mitarbeitende eine Website besuchen und zur Eingabe von Anmeldedaten aufgefordert werden, führt HP Sure Click Enterprise mit Hilfe des HP-Threat-Intelligence-Service im Hintergrund eine Sicherheits- und Domänen-Analyse durch. Wird die Website als sicher eingestuft, kann der Benutzer seine Anmeldedaten wie gewohnt eingeben. Handelt es sich jedoch um eine Phishing-Seite, erscheint ein Warnfenster. Je nach Konfiguration schließt sich anschließend die Micro-VM mit dem Browserfenster oder die Eingabefelder auf der Seite werden deaktiviert. In beiden Fällen bleiben die Zugangsdaten geschützt.

Alle Aktionen, die auf bekannten bösartigen und unseriösen Websites in der Micro-VM durchgeführt werden, werden ebenso an den Sure-Click-Controller gemeldet wie Malware-Aktivitäten, die von geöffneten Dateien ausgehen. So kann die IT-Abteilung jederzeit im Controller den Bedrohungsstatus überprüfen – und die Sicherheitsrichtlinien optimieren. HP Sure Click Enterprise ist somit eine wichtige Ergänzung zu Ihrer bestehenden Malware-Schutzlösung, da sie die derzeit erfolgreichsten Cyberangriffe wirkungslos macht.

SPRECHEN SIE MIT DEN EXPERTEN!

Lediglich zwei HP-Partner in Deutschland sind aktuell für die Sicherheitslösung HP Sure Click Enterprise zertifiziert: H&G gehört dazu. Vereinbaren Sie gern ein kostenfreies Beratungsgespräch mit unseren Experten.

Ihr Ansprechpartner
Karsten Janotta

Solution Consultant
+49 228 9080-784
karsten.janotta@hug.de

Drei Fragen an Heinz Mäurer

„DU KANNST AUF ALLES KLICKEN, WAS DU WILLST“

Heinz Mäurer, Sales Manager Security CE bei HP Deutschland, erklärt, wieso Isolationstechnologien eine kritische Lücke etablierter Security-Lösungen schließen.

Die Gefahren durch Malware in E-Mail-Anhängen oder Office-Dokumenten sind seit langem bekannt. Warum sind gerade solche Cyberangriffe noch so erfolgreich?

Ich habe lange Zeit einen großen Konzern betreut, der viel in Sicherheit investiert hat – nicht nur in Technologien, sondern auch in die Schulung der Mitarbeitenden. Die IT-Abteilung initiierte eine Phishing-Kampagne und warnte die Mitarbeitenden ausdrücklich vor einem erhöhten Aufkommen an Phishing-Mails. Wer eine verdächtige E-Mail erhalte, solle sie nicht öffnen, sondern an die Security weiterleiten. Drei Wochen später wurde testweise eine Phishing-Mail verschickt. Rund 40 Prozent klickten darauf. Das zeigt eindrücklich, dass Awareness-Kampagnen nie langfristig wirken. Hinzu kommt, dass Hacker sehr genau wissen, wie sie Menschen am besten dazu verleiten, Dateien zu öffnen oder auf Links zu klicken. In der Vorweihnachtszeit sind zum Beispiel oft gefälschte Benachrichtigungen per E-Mail von Paketdiensten im Umlauf – da kann es schnell passieren, dass jemand auf den Link klickt, ohne zu prüfen, ob dieser tatsächlich zu dem entsprechenden Dienst führt.

Das BSI empfiehlt Isolationstechnologien als eine sehr gute Möglichkeit, solche Angriffe zu verhindern. Was machen sie anders als bestehende Security-Lösungen?

Unser eigener Ansatz bei HP Sure Click Enterprise ist, dass wir den Anwendern vermitteln: Du kannst auf alles klicken, was du willst, und wenn es eine unbekannte nicht vertrauenswürdige Quelle ist, dann wird die Datei oder Website in einer isolierten Umgebung geöffnet. Dort kann sich die Malware nicht verbreiten. Für uns ist also nicht entscheidend, um welche Art von Schadsoftware es sich handelt, sondern woher sie kommt. In der isolierten Umgebung kann sie sich sogar entfalten, damit wir im Hintergrund beobachten können, was sie zu erreichen versucht und wie sie sich verbreitet. Diese Informationen können wir auf dem Dashboard aufbereiten und damit bestehende Sicherheitskontrollen ergänzen.

Heinz Mäurer,
Sales Manager Security CE
bei HP Deutschland

Viele werden jetzt denken: Brauche ich wirklich noch eine Sicherheitslösung, wenn ich bereits eine Antivirensoftware im Einsatz habe?

Die IT-Infrastruktur ist mit der vorhandenen Security-Software vor allem vor bekannter Malware relativ sicher. Aber es dauert in der Regel einige Tage, bis diese Lösungen eine neuartige Malware erkennen können. Zudem gibt es polymorphe Schadsoftware, bei der sich die Signatur ständig ändert. Das macht es den klassischen Security-Lösungen fast unmöglich, sie zu erkennen. Isolationstechniken wie HP Sure Click Enterprise sind hingegen nicht auf die Signatur angewiesen. Ich würde daher behaupten, dass typische Endpoint-Security-Lösungen mit Threat Detection 95 Prozent aller Probleme lösen. Mit unserer Lösung kommen noch einmal drei bis vier Prozentpunkte hinzu – und zwar genau in dem Bereich, in dem die meisten Angriffe erfolgreich sind. Da sollte man nicht am falschen Ende sparen, zumal Versicherungen zunehmend sagen, dass sie Cyberattacken nicht mehr abdecken werden, weil die Risiken unkalkulierbar sind.

Unser Flyer
„HP Sure Click Enterprise“
zum Download:

www.hug.de/FlyerSCE