Automated Monitoring

Warum Ihre digitale Identität kontinuierlichen Schutz braucht

united domains

Guide

Mehr Digitalisierung steht oft für Verbesserungen: mehr Effizienz, besseres Business und mehr Innovation. Leider gibt es aber auch unerwünschte Nebeneffekte. Die Bedrohung durch Cyber-kriminelle steigt in den vergangenen Jahren stetig. Unternehmen jeder Größe sind potenzielle Ziele für Angriffe, die nicht nur finanzielle Verluste, sondern auch im schlimmsten Fall erhebliche Reputationsschäden verursachen oder existenzbedrohend ausfallen können.

In diesem Guide erfahren Sie, warum es so wichtig ist, die digitale Identität zu schützen, warum Automated Monitoring ein unverzichtbares Werkzeug dafür ist und wie es funktioniert.

Was ist Automated Monitoring?

Automated Monitoring wartet nicht ab, bis etwas passiert, sondern beugt proaktiv vor. Das ist ein wichtiger Schritt der Veränderung, denn es ist wesentlich günstiger und smarter, Cyberangriffe zu verhindern, als ihre Schäden zu korrigieren (wenn es überhaupt möglich ist).

Automated Monitoring macht genau dies: **Es ist ein Frühwarnsystem, das Ihre Domains und damit verbundene Online-Präsenz kontinuierlich überwacht.** Es scannt das gesamte Internet nach potenziellen Bedrohungen, die Ihre Marke, Kunden oder Mitarbeiter gefährden könnten. Dabei werden im Fall des Dienstes von United Domains über 1,1 Millionen Domains ständig überwacht, um frühzeitig auf Gefahren aufmerksam zu machen.

Warum ist Automated Monitoring wichtig?

Stellen Sie sich vor, Sie sind der IT-Sicherheitsbeauftragte eines mittelständischen Unternehmens. Ihre Firma hat gerade eine erfolgreiche Produkteinführung hinter sich. Die Nachfrage steigt. Doch dann passiert es: Ein Kunde meldet, er sei auf eine verdächtige Website gestoßen, die der Ihrer Marke oder ihrem Produkt täuschend ähnlich sieht. Leider verfolgen solche Fake-Domains selten gute Absichten. So werden zum Beispiel von der falschen Domain entweder gefälschte Rechnungen verschickt oder Betrüger betreiben einen gefälschten Onlineshop.

Solche Szenarien sind leider keine Seltenheit – und sie verdeutlichen Folgendes: Es reicht heute nicht mehr, reaktiv vorzugehen, sondern proaktiver Schutz für die eigene Markenpräsenz ist wichtig und verhindert teure Folgen. Automated Monitoring bietet hier einen entscheidenden Vorteil: **Es erkennt früh potenzielle Bedrohungen, bevor sie sich zu ernsthaften Problemen entwickeln können**.

Dieser Schutz sieht so aus:

- Frühzeitige Erkennung von Domain-Registrierungen, die ein potenzielles Risiko für die Marke darstellen.
- Schutz vor Markenmissbrauch durch häufige Bedrohungen wie Fake-Domains.

Ein effektives Domain Monitoring hilft Unternehmen gleich dreifach, damit verbundene Geschäftsrisiken zu minimieren:

- Umsatzeinbußen durch Traffic-Diebstahl von ähnlichen Domains
- Imageschäden durch betrügerische Websites, die den Firmennamen missbrauchen
- Vermeidung rechtlicher Auseinandersetzungen und damit verbundener Kosten

Und wenn es doch zum Rechtsstreit kommt, helfen Ihnen spezialisierte Rechtsexperten. Sie können Maßnahmen wie Website-Takedowns, Unterlassungserklärungen und Streitbeilegungsverfahren effektiv und schnell umsetzen.

Jedes Unternehmen, jedes Produkt ist ein Ziel für Cybercrime

Mit jedem vernetzten Gerät und digitalisiertem Prozess, mit jeder Website und jedem Produkt wächst die Angriffsfläche für Cyberkriminelle. Und diese Straftäter werden immer raffinierter – denn Cyberkriminalität entwickelt sich zu einem äußerst lukrativen Geschäft. Und nicht nur Betreiber von Onlineshops sind im Fokus der Kriminellen: Phishing-Seiten, die Log-in-Formulare imitieren oder Falschinformationen verbreiten, treten immer häufiger auf.

Um die Dimension zu verdeutlichen: Cyberangriffe auf Unternehmen haben in den vergangenen zwölf Monaten (Stand August 2024) Schäden in Höhe von knapp 267 Milliarden Euro verursacht. Das geht aus einer Analyse des Digitalverbands Bitkom hervor. „Die Bedrohungslage für die deutsche Wirtschaft verschärft sich“, sagte Bitkom-Präsident Ralf Wintergerst gegenüber Handelsblatt. „Die Unternehmen müssen ihre Schutzmaßnahmen weiter hochfahren.“

Diese beeindruckende Summe erklärt die Motivation hinter solchen Angriffen: Sie versprechen ein gewinnbringendes Geschäft. 48 % der Unternehmen befürchten laut BKA, dass ein erfolgreicher Cyberangriff ihre Existenz bedrohen könnte. Besorgniserregend ist, dass trotz dieser wachsenden Bedrohung viele Unternehmen, insbesondere kleine und mittlere Unternehmen (KMU), noch keine ausreichenden Schutzmaßnahmen ergriffen haben.

Noch bedenklicher: Viele Unternehmen, insbesondere KMUs, wiegen sich in trügerischer Sicherheit, nach dem Motto „Ich bin zu klein, um Ziel eines Angriffs zu werden“ – eine Einschätzung, die angesichts der aktuellen Lage gefährlich sein kann. Denn laut Bundesamt für Sicherheit in der Informationstechnik (BSI) werden Cyberangriffe großflächig und automatisiert durchgeführt. „Es ist also höchste Zeit auch für KMU, die Informations- und Cyber-Sicherheit auf den neuesten Stand zu bringen und Mitarbeiterinnen und Mitarbeiter beim Gebrauch der Informationstechnik (IT) im Hinblick auf die gängigen Betrugsmaschen der Hacker regelmäßig zu sensibilisieren“, empfiehlt das Bundesamt auf seiner Webseite.

Welche Bedrohungen kann Automated Monitoring erkennen?

Unternehmen sind heute einer Vielzahl von digitalen Bedrohungen ausgesetzt. Hier einige Beispiele:

1. **Phishing-Angriffe:** Betrüger erstellen täuschend echte Kopien Ihrer Website, um sensible Daten von Ihren Kunden zu stehlen.
2. **Domain-Hijacking:** Kriminelle übernehmen die Kontrolle über Ihre Domain, oft durch Manipulation der Registrierungsdaten.
3. **Domain-Spoofing:** Ähnlich klingende Domainnamen werden als Fake-Domains registriert, um Ihre Kunden in die Irre zu führen. (Beispiel: statt www.beispieldomain.de wird www.beispildomain.de genutzt – nur ein fehlender Buchstabe, aber klingt ähnlich wie das Original)
4. **Typosquatting:** Angreifer registrieren Domains mit häufigen Tippfehlern Ihrer Marke, um vom Verkehr zu profitieren. (Beispiel: statt www.beispieldomain.de wird www.beispeildomain.de genutzt – und ein oft gemachter Buchstabendreher abgefangen)

Automated Monitoring kann all diese und weitere Bedrohungen frühzeitig erkennen und Sie warnen, bevor Schaden entsteht.

Domain Scan vs. Automated Monitoring: Was ist der Unterschied?

Viele Unternehmen verlassen sich nur auf sporadische Domain Scans, um potenzielle Bedrohungen zu erkennen. Doch während ein Domain-Scan nur eine Momentaufnahme liefert, bietet das Automated Monitoring einen kontinuierlichen, automatisierten Schutz. Hier ein detaillierter Vergleich, was dies im Einzelnen bedeutet:

Domain Scan:
- Einmalige Überprüfung
- Begrenzte Erkenntnisse
- Mögliche Lücken zwischen den Scans

Automated Monitoring:
- Kontrolle über Ihre Domain und Markeninhalte: Automated Monitoring überwacht und meldet alle bestehenden und neuen Registrierungen weltweit.
- Aufbereiteter Report: In regelmäßigen, individualisierbaren Intervallen erhalten Kunden einen Report mit allen identifizierten Übereinstimmungen ihrer Marke
- Beratung: Experten stehen bei jeder missbräuchlichen Domain-Registrierung oder bei Fremdnutzung des Brand-Contents zur Seite
- Rundum Überwachung: Es ist sowohl Domain-, als auch Content-Monitoring möglich

Fall 1: Eine fiktive Customer Success Story – So zahlt sich die Prävention aus

Wie sieht Automated Monitoring in der Praxis aus? Das verrät ein Blick auf die Erfahrungen eines fiktiven, aber typischen Kunden unseres Automated Monitorings: Nennen wir die Firma beispielhaft ExampleInnovate GmbH.

ExampleInnovate ist ein aufstrebendes mittelständisches Technologieunternehmen. Es entschied sich für Automated Domain Monitoring, um ihre wachsende Online-Präsenz zu schützen. In den ersten zwei Monaten blieb es ruhig – keine Auffälligkeiten wurden gemeldet. Schon im dritten Monat änderte sich das – und die Investition in Automated Domain Monitoring machte sich bezahlt. Das System entdeckte eine neu registrierte Domain, die der offiziellen ExampleInnovate-Website zum Verwechseln ähnlich war. Bei näherer Untersuchung stellte sich heraus, dass es sich um eine ausgeklügelte Phishing-Seite handelte, die darauf abzielte, sensible Kundendaten zu stehlen. Dank der prompten Warnung durch unser Monitoring-System konnte ExampleInnovate schnell reagieren:

1. Die betrügerische Website wurde innerhalb von 24 Stunden entfernt.
2. Kunden wurden proaktiv über den Vorfall informiert, was das Vertrauen in die Marke stärkte.
3. Potenzielle Datenverluste und Rufschädigung wurden verhindert.
4. Das Unternehmen konnte einen möglichen Verlust von Bestandskunden abwenden.

Ohne das kontinuierliche Monitoring hätte der Kunde die Bedrohung möglicherweise erst bemerkt, wenn es zu spät gewesen wäre. Die Investition hat sich somit mehr als ausgezahlt.

Fall 2: Warum zusätzlich Content Monitoring noch mehr Sicherheit schafft

Die ExampleSportStyle, (ein ebenfalls fiktives) aufstrebendes Unternehmen im Bereich Sportbekleidung, hatte bereits positive Erfahrungen mit Automated Domain Monitoring gemacht. Es hatte dem Hersteller geholfen, mehrere Fälle von Typosquatting zu identifizieren und zu unterbinden. Doch der wahre Durchbruch kam, als ExampleSportStyle sich entschied, zusätzlich unser Content Monitoring zu nutzen. Der Auslöser war die Einführung ihrer neuen (fiktiven) Premium-Laufschuhlinie „ExampleRunning Pro 2024“.

Unter einer per Zufallsgenerator erzeugten Domain erschien ein Fake-Shop, der mit Domain Monitoring nicht erkannt worden wäre, da der Name “xyz2312-shop.com” nichts mit dem Markennamen zu tun hat. Leider wurden auch noch Phishing-Emails verschickt, die täuschend echt einen Newsletter der Firma imitierten und dann per Link zu einem Sonderangebot in dem Fake-Shop leiteten. Die Kunden fokussierten sich auf den Inhalt und bemerkten so die falsche Domain in der Browser-Adresszeile nicht.

Das Content Monitoring erkannte, dass große Teile des Textes und der Produktbeschreibungen direkt von der offiziellen SportStyle-Website kopiert worden waren. Zudem wurden Bilder der echten „ExampleRunning Pro 2024“ Schuhe verwendet, aber zu deutlich niedrigeren Preisen angeboten.

Dank der kombinierten Kraft von Domain- und Content-Monitoring konnte SportStyle schnell reagieren. Der Geschäftsführer von ExampleSportStyle zeigte sich begeistert: „Anfangs dachten wir, das Automated Domain Monitoring würde ausreichen. Aber das Content Monitoring hat uns vor einem viel subtileren, schwer erkennbaren und potenziell schädlicheren Angriff bewahrt. Die Investition hat sich mehrfach ausgezahlt.“

Der entscheidende Unterschied: Die Kraft der Kontinuität

Das fiktive Beispiel unterstreicht die Bedeutung der Kontinuität beim Automated Monitoring. Eine gelegentliche Überprüfung reicht heute nicht mehr aus. Bedrohungen können jederzeit auftauchen und jede Verzögerung in der Erkennung kann kostspielige Folgen haben. Spam- oder Phishingschutz sind auch kein Ersatz. Damit sind lediglich interne Mitarbeiter geschützt, nicht aber Kunden und Geschäftspartner.

Mit Automated Monitoring setzen Sie auf:

- **24/7 Überwachung:** keine Lücken, keine blinden Flecken.
- **Schnelle Reaktionszeiten:** Bedrohungen werden erkannt, bevor sie sich auswirken können.
- **Präventiver Ansatz:** Potenzielle Gefahren werden identifiziert, bevor sie zu echten Problemen werden.
- **Expertenunterstützung:** Unser Team steht Ihnen bei der Bewertung und Bewältigung von Bedrohungen zur Seite.

Automatisierung heißt auch Zeit sparen. Wichtig zu wissen ist, dass Automated Monitoring im Allgemeinen keine weitere Belastung oder großen Zeitaufwand, sondern eine Entlastung für Sie darstellt. Kunden von United Domains verbringen im Schnitt weniger als 15 Minuten damit – zum Beispiel beim Lesen des Reports. Und wenn es Fragen gibt, etwa bei kritischen Ergebnissen im Report, hilft ein kostenloses und unverbindliches Beratungsgespräch mit einem Online Brand Protection Experten, um, wenn notwendig, die nächsten Schritte zu besprechen.

Maßgeschneidertes Monitoring für jeden Bedarf

Ob Sie ein kleines Unternehmen sind, das gerade erst seine digitale Identität aufbaut, oder ein großes Unternehmen mit komplexen Markenportfolios – es gibt die richtige automatisierte Monitoring-Lösung.

Automated Domain Monitoring: Automated Domain Monitoring überwacht kontinuierlich Domain-Registrierungen und -Änderungen. Es ist besonders effektiv für Unternehmen, die ihre Marke im Domain-Bereich schützen möchten. Automated Domain Monitoring erkennt Typosquatting, Domain-Spoofing und ähnliche Bedrohungen, die auf der Domain-Ebene auftreten.

Automated Content Monitoring: Automated Content Monitoring geht über die Domain-Ebene hinaus und überwacht Webinhalte auf spezifische Schlüsselwörter oder Themen. Diese Lösung ist besonders effektiv bei der Erkennung von Copycat-Websites, Fake-Shops und unbefugter Verwendung Ihrer Markeninhalte, unabhängig von der verwendeten Domain.

Kombiniertes Domain- und Content Monitoring: Automated Domain Content Monitoring vereint die Funktionen von Domain Monitoring und Content Monitoring zu einer umfassenden Lösung. Es bietet einen ganzheitlichen Schutz, der sowohl Domain-basierte als auch inhaltliche Bedrohungen abdeckt. Diese Option ist ideal für Unternehmen, die einen vollständigen Überblick über ihre Online-Präsenz benötigen und maximalen Schutz anstreben.

Managed Automated Monitoring: Managed Automated Montoring ist ein vollständig verwalteter Monitoring-Service, der sowohl Automated Domain Monitoring und Automated Content Monitoring umfassen kann. Bei dieser Option übernimmt ein Expertenteam die kontinuierliche Überwachung, Analyse und Berichterstattung. Kunden werden proaktiv über potenzielle Bedrohungen informiert und erhalten konkrete Handlungsempfehlungen. MAM eignet sich besonders für Unternehmen, die maximalen Schutz bei minimalem internem Aufwand wünschen.

Noch Fragen? Wir helfen ihnen auch die perfekte Lösung für ihr Unternehmen zu finden.

Fazit: Der wichtigste Kontaktpunkt zu Kunden, kontinuierlich sicher

Ihre Online-Präsenz ist der erste (und wichtigste) Kontaktpunkt zu Ihren Kunden. Somit ist der Schutz Ihrer Domain mehr als nur eine IT-Aufgabe – es ist eine strategische Notwendigkeit. Automated Monitoring bietet Ihnen die Sicherheit, die Sie brauchen, um sich auf Ihr Kerngeschäft zu konzentrieren. Es ist nicht nur ein Werkzeug, sondern ein digitaler Wächter, der ununterbrochen für Sie im Einsatz ist. Der beste Rat ist aber: Warten Sie nicht, bis es zu spät ist. Aktivieren Sie noch heute Automated Monitoring, um auch Ihr Unternehmen zu schützen. Denn im Internet gilt: Vorbeugen ist besser als Heilen.

So aktivieren Sie Automated Monitoring

Automated Monitoring aktivieren Sie in wenigen Minuten selbst in unserem Monitoring Konfigurator. Dort geben Sie zu überwachende Begriffe und Domains ein und wählen, ob Domain und Content (oder beides) überwacht werden sollen. Zudem geben Sie eine E-Mail an, an die regelmäßige Reports geschickt werden sollen – und das Intervall, in dem Sie die Reports erhalten möchten. Das Monitoring ist monatlich kündbar, so können Sie das Automated Monitoring risikolos testen.

Über united-domains

united-domains ist ein etablierter Domain-Registrar und Anbieter von Webhosting-Diensten. Mit Sitz in Deutschland bieten wir professionelle Lösungen für Domainregistrierung, Web-Präsenz-Management und sichere Markendomains. Zu unseren Kunden gehören viele der bekanntesten Marken. Diese schätzen unsere Domainexpertise, unsere hohen technischen Standards sowie den united-domains Kundenservice, der Unternehmen auch bei komplexen Domainanforderungen stets zuverlässig weiterhilft.

Impressum
united-domains GmbH, Gautinger Straße 10, 82319 Starnberg, Deutschland. E-Mail support@united-domains.de, Telefon +49 (0) 8151 / 36867-0. HRB 29 43 48, Amtsgericht München. USt.-IdNr. DE203066334, MwSt. Schweiz: CHE-274.284.535 MWST, Türkei: 8920484983. Geschäftsführung Saad Daoud, Michael Klemund

Die Inhalte des White Papers wurden mit größter Sorgfalt erstellt. Für Richtigkeit, Vollständigkeit und Aktualität keine Gewähr.

© united-domains, 2024. Alle Rechte vorbehalten – einschließlich der, welche die Vervielfältigung, Bearbeitung, Verbreitung und jede Art der Verwertung der Inhalte dieses Dokumentes oder Teile davon außerhalb der Grenzen des Urheberrechtes betreffen. Handlungen in diesem Sinne bedürfen der schriftlichen Zustimmung durch united-domains. united-domains behält sich das Recht vor, Aktualisierungen und Änderungen der Inhalte vorzunehmen.