WHITEPAPER

CYBER-SICHERHEIT FÜR IHRE DOMAIN

IN 3 SCHRITTEN DIE EIGENE WEBSITE SICHERN

Domain Factory

CYBER-SICHERHEIT FÜR IHRE DOMAIN

Wer sich als Unternehmer oder Selbstständiger eine Domain gesichert und registriert hat, meint in der Regel, damit sei der wichtigste Schritt der Online-Arbeit erledigt? Dieser Irrglaube führt häufig dazu, dass sich Betreiber von Webseiten in Sicherheit wiegen und sich nicht weiter mit potenziellen Gefahren beschäftigen. Dabei können diese jeden treffen, der eine Webseite betreibt. Allein im Jahr 2020 bezifferte sich der Schaden durch **Cyberkriminalität auf 88 Millionen Euro**. Tendenz: steigend.

Eine weit verbreitete Form der Online-Kriminalität ist die **Domainpiraterie**, auch bekannt als **Domaingrabbing**. Kriminelle sichern sich dabei Domains, die zum Beispiel geschützte bzw. genutzte Marken-, Personen und Unternehmensnamen enthalten.

Auch erkennbare Markennamen mit eingebauten Vertippern sind gern genutzte Adressen, die verheerende Konsequenzen für die Sichtbarkeit im Web haben können. Denn: Der Kunde, der Dienstleistungen und Produkte per Klick kaufen möchte, weiß nicht, wer für den Webauftritt verantwortlich ist. Im schlimmsten Fall leidet die Online-Reputation, das Image nimmt Schaden und es wirkt sich auf Umsätze aus dem Online sowie analogen Handel aus. Dabei ist Domainpiraterie gerade aktuell weit verbreitet.

Ein weiteres Risiko, sind **Expired Domains**. So werden Domains bezeichnet, die in Kürze gelöscht werden oder bereits gelöscht worden sind. Wenn die Registrierung einer betriebenen Website ausläuft, sollten Sie diese verlängern. Ansonsten bestünde die Gefahr des sogenannten **Domainsnappings** – die Registrierung kurz nachdem eine Domain freigegeben wurde.

Eine noch weniger bekannte, aber dennoch wichtig zu beachtende Methode der Cyberkriminalität ist das **Domain-Spoofing**: Hierbei handelt es sich um einen virtuellen Trickbetrug. Kriminelle nutzen einen scheinbar seriösen Webauftritt, um User direkt zu kontaktieren und personenbezogene Daten (z.B. Kreditkartendaten oder Anmeldedaten für ein Bank-Konto) zu erhalten. Nutzer bemerken dabei nicht, dass sie diese vertraulichen Daten in die Hände von Kriminellen geben. Im schlimmsten Fall kann die Kundenvertrauensbasis durch derartige Vorfälle dauerhaft beschädigt sein.

Der aktuelle Umgang mit dem Domainmanagement zeigt, dass dringender Handlungsbedarf besteht.

MEHR ALS JEDES ZEHNTE UNTERNEHMEN WAR SCHON EINMAL OPFER VON DOMAINPIRATERIE

MIT DIESEN SCHRITTEN SCHÜTZEN SIE SICH:

- → Domains nach einer klaren **Domainstrategie** einsetzen
- → ein umfangreiches **Domainportfolio** etablieren
- → regelmäßiges **Monitoring** der eigenen Domains
- → **Sicherheitsberatung** durch Ihren Domain-Anbieter

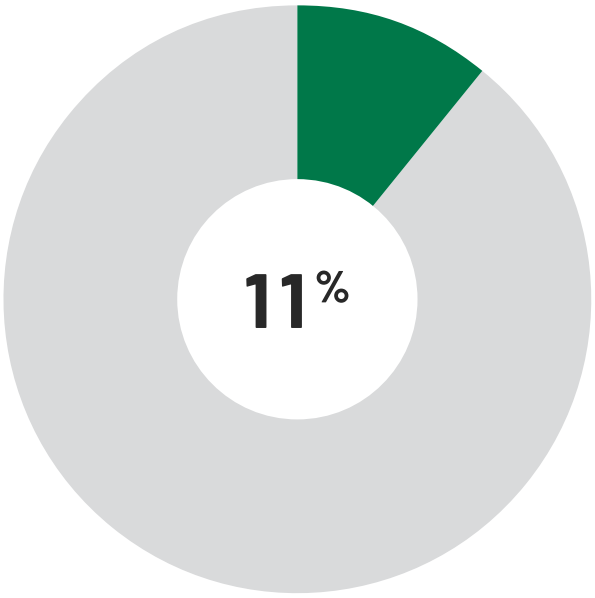
Welche Formen von Domainpiraterie gibt es?

Domain-Spoofing/Phishing, Missbrauch des Markenrechts, Domaingrabbing, Typosquatting, Cybersquatting, Reverse Domain Hijacking, Domain Snapping/Missbrauch von Expired Domains uvm.

Mehr dazu:
https://www.df.eu/blog/zukunftsstrategien-domains-download/
Eine Studie von DomainFactory in Zusammenarbeit mit YouGov® Marktforschung

35% DER BEFRAGTEN UNTERNEHMEN HABEN NOCH NIE ETWAS VON DOMAINPIRATERIE GEHÖRT

Laut der aktuellen Studie von DomainFactory* in Zusammenarbeit mit dem Marktforschungsinstitut YouGov waren **elf Prozent** der befragten Unternehmen und Selbstständigen bereits von Domainpiraterie **betroffen**. Beunruhigend: Ein Drittel der Befragten hat noch nie etwas von Domainpiraterie gehört. Insbesondere Selbstständige (45 Prozent) wollen sich anscheinend nicht mit der möglichen Gefahr auseinandersetzen. Doch das muss nicht sein. Jeder kann durch eigenes Handeln für deutlich mehr Sicherheit der eigenen Website sorgen. In diesem Whitepaper erfahren Sie, wie Sie Ihre Domain in drei Schritten schützen und somit auch Ihre Umsätze langfristig sichern.



11 % waren schon Opfer von Domainpiraterie.

Mehr als jedes zehnte Unternehmen war bereits Opfer von Domainpiraterie.

Jedes Jahr nehmen **Cyberattacken auf Unternehmen** zu. Allein 2020 bezifferte sich der Schaden durch Cyberkriminalität in Deutschland auf **88 Millionen Euro**. Bislang sind Solo-Selbstständige seltener davon betroffen, aber auch nur wenig mit dem richtigen Domainmanagement vertraut.

*** Hier geht's zur gesamten Studie:**
https://www.df.eu/blog/zukunftsstrategien-domains-download/

STEP 01 — DIE DOMAIN-STRATEGIE

Eine Domain kaufen Sie in der Regel in wenigen Klicks ganz unkompliziert. Doch auch danach sollten sich Unternehmen, Selbstständige und Shop-Anbieter mit ihrer Domain befassen.
Sie wird sowohl von Selbstständigen als auch von größeren Unternehmen häufig stiefmütterlich behandelt und ist doch das Fundament für langfristigen Erfolg und Sicherheit: Die passende Domainstrategie. Der Domainname ist die Basis, auf der die Strategie fußt. Es lohnt sich also auch zum Start einer Online-Seite bereits Zeit und Kreativität in den Domainnamen zu investieren.

Der Blick in die Zukunft ist in Sachen Domain mindestens genauso relevant wie beispielsweise eine jährlich aufgestellte Marketing-Strategie. Die Inhalte werden an aktuelle Unternehmensziele und die Bewegungen am Markt angepasst. Entsprechend kann und sollte auch das Domainportfolio weiter ausgebaut werden.

STEP 02 — DAS DOMAIN-PORTFOLIO

Viel hilft viel? Online ist dieses Credo tatsächlich hilfreich. In regelmäßigen Abständen werden neue Domainendungen am Markt etabliert. .com und .de sind vielleicht die bekanntesten, doch wussten Sie, ...

- → ***...dass Sie Ihre Domain auch internationaler mit einer .eu-Endung oder inhaltlicher mit einer .info-, .gmbh- oder .shop-Endung aufstellen können?***
- → ***...dass Sie, auch verschiedene Produkt- und/oder Kampagnenzusätze im eigentlichen Domainnamen mitbedenken können?***
- → ***...dass auch bewährte Suchbegriffe rund um Ihre Marke können ein Indiz sind, um das Domainportfolio auf ein sicheres Fundament zu stellen?***

STEP 03 — VERTRAUEN IST GUT, KONTROLLE IST BESSER

Regelmäßiges Monitoring der eigenen Keywords hilft, den Überblick zu behalten. Dadurch können Duplikate mit Vertippern und artverwandte Plagiate schnell aufgedeckt und Markenmissbrauch vermieden werden.

- → ***Finden Sie nur Ihre eigenen Domains oder tauchen Domains mit Ihrem Markennamen und fremden Inhalten bei den Suchmaschinen auf?***
- → ***Landen Sie einen Suchtreffer, der sich verdächtig Ihrem eigenen Markennamen nähert?***
- → ***Finden Sie Domains, die Ihren Markennamen nutzen und nur mit einem Tippfehler versehen sind?***

Wenn Sie per Monitoring auf Domainpiraterie aufmerksam werden, ist schnelles Handeln gefordert.

OPFER VON DOMAINPIRATERIE – WAS TUN?

Haben Sie bei Ihrem monatlichen Monitoring festgestellt, dass Sie von Domainpiraten angegriffen werden, behalten Sie einen kühlen Kopf! Mit einem systematischen Vorgehen ist der Schaden schnell begrenzt.

Zunächst recherchieren Sie, in welchem Verzeichnis die betroffene Domain bzw. das Plagiat registriert ist. Anschließend sperren Sie diese. Eine solche Sperrung kann für .de-TLD bei der **DENIC** (Abkürzung für: **D**eutsches **N**etwork **I**nformation **C**enter) beantragt werden. Die DENIC betreibt und verwaltet die .de-Endung[1] und ist in solchen Fällen der wichtigste Ansprechpartner. Welche Registry für welche Domain verantwortlich ist, ist immer aktuell unter dem folgenden Link nachzulesen: www.ntldstats.com

Wichtige Tipps und eine professionelle Beratung, was Unternehmen und Selbstständige bei der Domainregistrierung unbedingt beachten sollten, gibt das Domain-Team von DomainFactory:

→

Tel +49.89 998 288.031
E-Mail vertrieb@df.eu

Hier geht's zur gesamten Studie:
https://www.df.eu/blog/zukunftsstrategien-domains-download/

[1] https://www.denic.de/ueber-denic/aufgaben/