HÄUFIG GESTELLTE FRAGEN ZU CYBER

Gryves als Gesellschaft

Wer ist Gryves?

Gryves ist eine unabhängige, im Besitz des Managements befindliche FinTech Company, die eine Reihe von Cybersicherheitsdiensten und Risiko Management Aktivitäten anbietet. Neben den beiden Assessments für den KMU-Markt ('DOMAIN CYBER CHECK' und 'BUSINESS BASIC CYBER CHECK') verfügt Gryves auch über spezialisierte Angebote für Versicherungen und Banken.

Gryves Assessment Services für KMUs

Welche Assessment Services bietet Gryves für KMUs an?

Um Unternehmen rasch und einfach aufzuzeigen, wie sie sich einerseits im digitalen Umfeld präsentieren und andererseits wie sie firmenintern organisatorisch gegen Cyberrisiken aufgestellt sind, bietet Gryves ein zweistufiges, sich ergänzendes Assessmentmodell an.

'DOMAIN CYBER CHECK'

Was ist ein DOMAIN CYBER CHECK?

Der DOMAIN CYBER CHECK ist ein domainbasiertes Assessment, das anhand von wenigen Angaben über das Unternehmen (Domain, Branche, Domizilland, Grösse – Umsatz und Anzahl Mitarbeitende) einen konkreten Überblick über den digitalen Fussabdruck, das digitale Gefährdungspotenzial sowie zu möglichen Cyberschwachstellen gibt.

Welche Daten verwendet Gryves für die Domain basierten Assessments sowie für die Berechnungen?

Gryves sammelt die durch die tägliche Nutzung des Internets oder von E-Mails anfallenden digitalen Spuren und kombiniert diese mit den Daten aus verschiedenen öffentlich zugänglichen Datenbanken, und wertet und verarbeitet all dies mit Hilfe von künstlicher Intelligenz.

Welche Resultate liefert der DOMAIN CYBER CHECK?

Die Resultate des DOMAIN CYBER CHECKs werden in einem Bericht zusammengefasst. Dieser zeigt zwei Kernkennzahlen und eine Auflistung festgestellter ‘Findings’ und möglicher Schwachstellen.

Wofür stehen die beiden Kennzahlen im Bericht?

Cyberrisiko Gefährdung: Wahrscheinlichkeit mit der eine Firma in den nächsten 12 Monaten von einem Cyberschadensereignis betroffen sein könnte.
Wahrscheinlichkeit, dass ein Cyberangriff zu einem Betriebsunterbruch führt.

Was bedeuten die Farben in den Feldern der Kennzahlen?

Die Kennzahlen werden in einem Ampelsystem dargestellt, wobei gelb oder rot auf ein erhöhtes Risiko hinweisen.

Was beschreiben die 'Findings' im Bericht?

Die 'Findings' im Report des DOMAIN CYBER CHECKs stellen die während dem Assessment gewonnenen Erkenntnisse dar. Findings, die bewusst konfigurierte Systemeinstellungen bei einer Firma darstellen, sind kein Problem. Solche jedoch, die nicht bewusst so eingestellt wurden oder von denen das Unternehmen keine Kenntnisse hat, können eine konkrete Schwachstelle und ein Sicherheitsrisiko darstellen.

Wie lange dauert es, bis ein DOMAIN CYBER CHECK durchlaufen ist?

Es braucht nicht mehr als fünf Minuten.

Kann für den DOMAIN CYBER CHECK ein Abonnement abgeschlossen werden?

Ja, der DOMAIN CYBER CHECK kann einzeln sofort als auch in Form eines Abonnements von drei (eine Sofortbewertung und zwei innerhalb von 12 Monaten) oder sechs Bewertungen (eine Sofortbewertung und fünf innerhalb von 24 Monaten) erworben werden.

Datensicherheit

Wer hat Zugriff auf die von Gryves erstellten Berichte und Ergebnisse?

Nur der Benutzer, der den Bericht bestellt hat, hat Zugriff darauf. Ein Benutzer muss über eine gültige E-Mail-Adresse verfügen, die mit der Domain übereinstimmt, für die ein Assessment bestellt wird.

Welche Vorkehrungen sind vorgesehen, um sicherzustellen, dass kein unbefugter Benutzer Zugriff auf die sensiblen Daten hat?

Eine 2-Faktor-Authentifizierung mit einer Verifizierungs-E-Mail.

Wie schützt und verwendet Gryves die Daten von Unternehmen?

Gryves anerkennt, dass Informationssicherheit ein integraler Bestandteil des Datenschutzes ist. Obwohl keine Datenübertragung (auch nicht über das Internet oder eine Website) als 100% einbruchsicher gewährleistet werden kann, hat Gryves eine Reihe wirtschaftlich sinnvoller physischer, technischer und verfahrenstechnischer Massnahmen ergriffen, um personenbezogene Daten gemäss den datenschutzrechtlichen Anforderungen vor unbefugtem Zugriff, Nutzung, Offenlegung, Änderung oder Vernichtung zu schützen.

Erfüllt Gryves die Anforderungen der EU GDPR?

Ja, was die GDPR in Bezug auf die von uns verwendeten Daten betrifft, befolgen wir die Regeln der GDPR.

Allgemeines

Worin besteht der Unterschied zwischen ausserhalb und innerhalb der Firewall?

Gryves' DOMAIN CYBER CHECK bewertet den digitalen Fussabdruck des Unternehmens ausserhalb seiner Firewall, indem ausschließlich auf öffentlich zugängliche Daten zugegriffen wird. Gryves dringt zu keinem Zeitpunkt in die Systeme der bewerteten Unternehmen ein und hat keinen Zugriff auf deren Daten.

Gryves Limited, Seestrasse 25, 8810 Horgen, Schweiz.
20. Dezember 2018

Was ist ein Cyberrisiko?

Risiken, die sich aus jeder Form von digitalen Angriffen ergeben, denen jeder Nutzer der Informations- und Kommunikationstechnologie ausgesetzt ist, welche die Vertraulichkeit, Verfügbarkeit oder Integrität von Daten oder Diensten gefährden, Lösegeldforderungen oder sogar Wirtschaftsspionage beinhalten. Die Beeinträchtigung der operativen Systeme kann schliesslich zu Betriebsstörungen, (kritischen) Infrastrukturausfällen oder Sachschäden an Menschen und Eigentum führen und zu finanziellen Verlusten und Störungen oder zu Reputationsschäden des Unternehmens führen.

Cyberrisiken sind nicht nur Sache des IT-Teams, auch wenn diese vor allem direkt involviert sind. Cyberrisiken können auch durch die in und für ein Unternehmen tätigen Personen, durch nicht adequate, interne Arbeitsabläufe und -verfahren sowie durch die zugrundeliegende Technologie und Frontausrichtung verursacht werden.

Dementsprechend muss sich auch das (Risiko-)Management des Unternehmens regelmässig mit diesem Thema befassen und ein Verständnis für die sich ständig ändernden Risiken entwickeln.

Wo finde ich unabhängige Informationen zum Thema Cyberrisiko?

Es gibt eine Reihe von Websites, auf denen einige aktuelle Informationen über Cyberrisiken zu finden sind. In einigen Ländern unterhalten Regulierungsbehörden oder ihnen nahe stehende Organisationen solche Websites, z.B. http://securityaffairs.co/wordpress/ oder https://www.melani.admin.ch/melani/de/home/themen.html.

Darüber hinaus gibt es viele verschiedene Standards, die den Bedarf an zusätzlichen Informationen decken können, z. B. ISO 27000ff, NIST, NATO-Cyber-Standard.