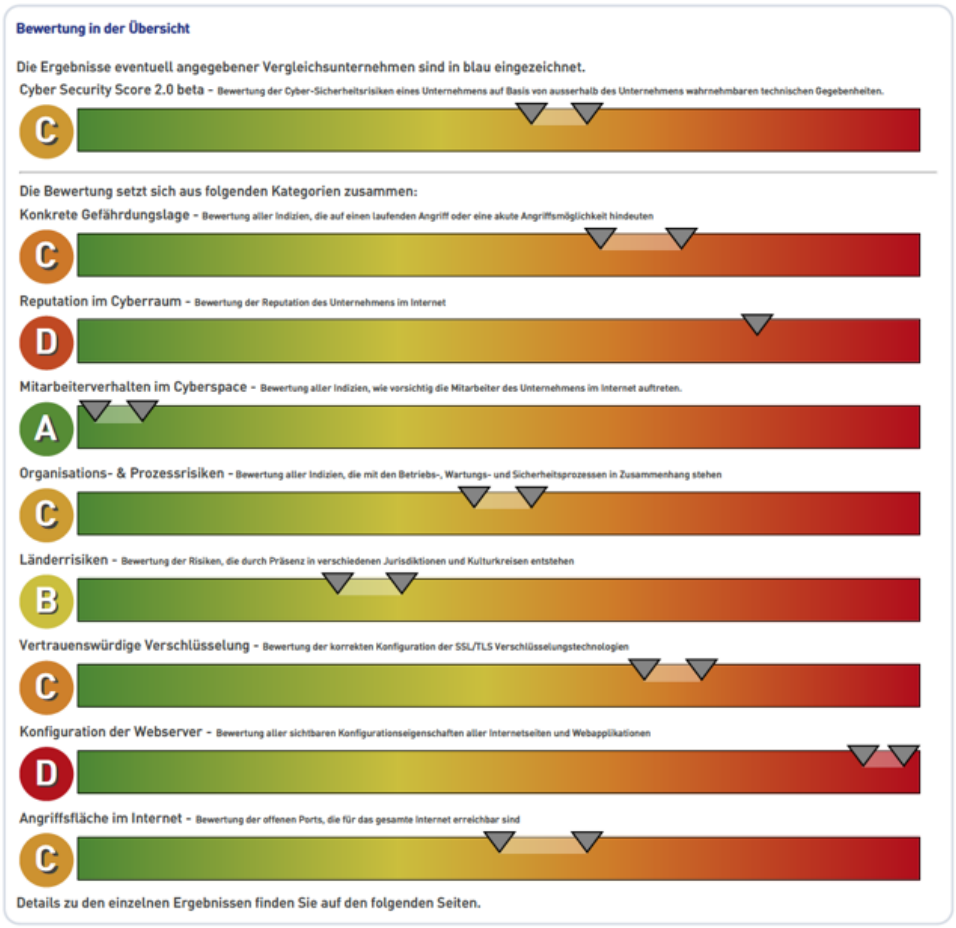
„Ihr digitaler Fußabdruck im Netz“

Open Source Intelligence (**OSINT**) ist ein Begriff aus der Welt der Nachrichtendienste, bei dem für die Nachrichtengewinnung Informationen aus frei verfügbaren, offenen Quellen gesammelt werden, um durch Analyse der unterschiedlichen Informationen verwertbare Erkenntnisse zu gewinnen. Dabei werden frei zugängliche Medien genutzt und die Ergebnisse systematisch zusammengefasst.



Die DQS BIT bietet eine auf die Belange der ISO 27001 angepasste Methode des CyDIS-Scorings an, die Ihnen die Möglichkeit gibt diese Erkenntnisse als technischen Auditbericht zu nutzen. Im Unterschied zu herkömmlichen PENTESTS enthält dieser Bericht auch Erkenntnisse über bereits abgeflossene Informationen und nicht nur über potentielle Sicherheitslücken. Da Informationssicherheit nicht nur von technischen Maßnahmen abhängt – 85% aller ungewollten Informationsabflüsse in Unternehmen gehen auf den Faktor Mensch zurück – liefert unser Bericht auch Erkenntnisse zu bereits „verlorenen“ gegangenen Informationen, wie z.B. User Credentials.

Vertrauen reicht nicht aus - Wissen hilft weiter, schnell, einfach, diskret

*nach dem CyDIS Scoring

SIE HABEN SCHON VIEL VON INFORMATIONSSICHERHEIT GEHÖRT – SIND SICH ABER NICHT SICHER, OB IHR UNTERNEHMEN RICHTIG AUFGESTELLT IST?

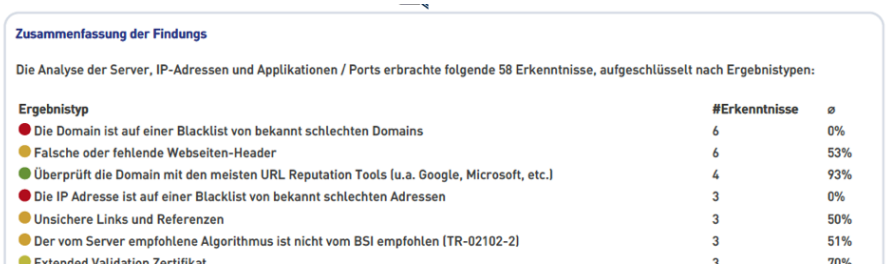
Zum Einsatz kommen ungefähr 5000 Softwaretools, die die Spuren Ihres Unternehmens im Netz analysieren und zur ISO 27001 in den Kontext setzen. Sie erhalten einen Bericht, den wir in zwei Qualitätsstufen anbieten:

- **27001OSINT PRE : Management Overview – First Look**
- **27001OSINT PRE+ : Detailbericht auf Grundlage der ISO 27001 Anforderungen**
- **Zusatzmodul: OSINT Audit**

Wir bieten Ihnen die Möglichkeit über einen **PreCheck (OSINT PRE)** Ihren „digitalen Fußabdruck“ im Netz zu erfahren – Schwachstellen und Stärken in Bezug auf die führende Norm im Bereich der Informationssicherheit ISO 27001 werden Ihnen aufgezeigt. Sie erhalten den Bericht in elektronischer Form und haben die Möglichkeiten diesen in Ihrem Unternehmen weiter zu verarbeiten. Oder Sie möchten wissen, wie es um Ihre **Partner oder Lieferanten** steht – kein Problem – der Bericht **27001OSINT PRE** eignet sich auch hervorragend für dieses Einsatzgebiet – die genutzten Quellen sind öffentlich zugänglich – es bedarf hierzu keiner Genehmigung.

Zusätzlich zum Report **27001 OSINT PRE+** haben Sie die Möglichkeit durch die Erläuterung unserer jahrelang erfahrenen Auditoren aus dem Bereich Informationssicherheit einen optimalen Startpunkt für die Einführung und Zertifizierung eines Managementsystems Informationssicherheit nach ISO 27001 zu erhalten (OSINT PRE+).

Der Bericht **27001OSINT PRE+** kann mit einer Vorstellung der Ergebnisse in Ihrem Hause durch einen erfahrenen Auditor ergänzt werden (**OSINT Audit).** Durch das Mapping zur ISO 27001 haben Sie die Möglichkeit, direkt die Schwachstellen im Bereich der Informationssicherheit an den Vorgaben der führenden Norm zu Informationssicherheit, der ISO 27001 zu bewerten.

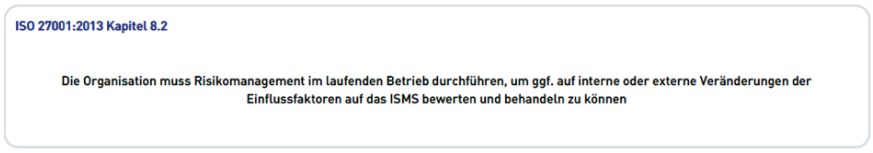


Zusammenfassung der Findings

Die Analyse der Server, IP-Adressen und Applikationen / Ports erbrachte folgende 58 Erkenntnisse, aufgeschlüsselt nach Ergebnistypen:

Ergebnistyp	#Erkenntnisse	ø
Die Domain ist auf einer Blacklist von bekannt schlechten Domains	6	0%
Falsche oder fehlende Webseiten-Header	6	53%
Überprüft die Domain mit den meisten URL Reputation Tools (u.a. Google, Microsoft, etc.)	4	93%
Die IP Adresse ist auf einer Blacklist von bekannt schlechten Adressen	3	0%
Unsichere Links und Referenzen	3	50%
Der vom Server empfohlene Algorithmus ist nicht vom BSI empfohlen (TR-02102-2)	3	51%
Extended Validation Zertifikat	3	70%

Die entsprechenden Normkapitel werden Ihnen angezeigt und Sie erhalten den Hinweis, wie Sie Schwachstellen systematisch vermeiden können.



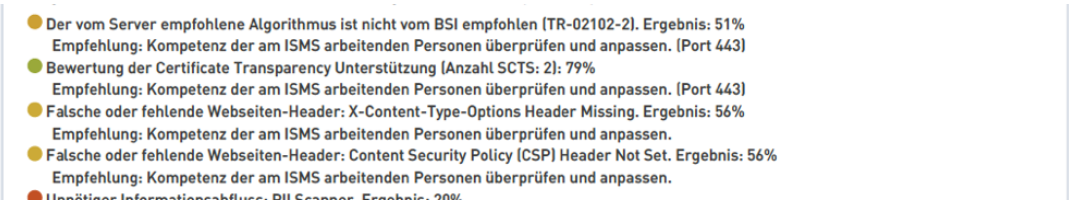
ISO 27001:2013 Kapitel 8.2

Die Organisation muss Risikomanagement im laufenden Betrieb durchführen, um ggf. auf interne oder externe Veränderungen der Einflussfaktoren auf das ISMS bewerten und behandeln zu können

*nach dem CyDIS Scoring

SIE SIND BEREITS NACH ISO 27001 ZERTIFIZIERT? SIE MÖCHTEN TECHNISCH DIE SICHT AUF DIE ISO 27001 VERTIEFEN UND ÜBER IHR AUDIT HINAUS SCHWACHSTELLEN ERKENNEN?

Wir bieten Ihnen die Möglichkeit über einen **PostCheck (OSINT POST)** Ihren „digitalen Fußabdruck“ im Netz zu visualisieren – Der Reifegrad in Bezug auf die Umsetzung der führenden Norm im Bereich der Informationssicherheit ISO 27001 wird Ihnen aufgezeigt.



Zusätzlich zu diesem Report ISO 27001 POST haben Sie die Möglichkeit durch die Erläuterung unserer jahrelang erfahrenen Auditoren aus dem Bereich Informationssicherheit weitere Ansatzpunkte für die Verbesserung der Wirksamkeit Ihres ISMS nach ISO 27001 zu erhalten. Zum Einsatz kommen ungefähr 5000 Softwaretools, die die Spuren Ihres Unternehmens im Netz analysieren und zur ISO 27001 in den Kontext setzen.

Sie erhalten einen Bericht, den wir zwei zeitlichen Ausprägungen anbieten:

- **27001OSINT POST**
- **27001OSINT CONT**
- **Zusatzmodul: OSINT Audit**

Der Bericht **27001OSINT POST** kann mit einer Vorstellung der Ergebnisse in Ihrem Hause durch einen erfahrenen Auditor ergänzt werden (**OSINT Audit).** Durch das Mapping zur ISO 27001 haben Sie die Möglichkeit, direkt die Schwachstellen im Bereich der Informationssicherheit mit den Vorgaben Ihres Managementsystems nach ISO 27001 zu matchen. Dies kann als direkter Input für Ihren Schwachstellenmanagementprozess genutzt werden. Die ISO 27001OSINT Berichte bieten Ihnen also eine sinnvolle Ergänzung, um Themen aus Ihrem Zertifizierungsaudit nach ISO 27001 zu vertiefen und technisch nochmals detailliert zu hinterfragen.

Sie möchten auf dem Laufenden bleiben? Wir bieten Ihnen ein Jahres-ABO mit einem quartalsweisen Berichts-Abo **(27001OSINT CONT)** Sie erhalten 4 Berichte zum Preis von drei Berichten. Im ersten Jahr bieten wir Ihnen dazu kostenfrei ein **„Alerting“** sollten sich Ergebnisse unserer Prüfung sich wesentlich verändern. Sie müssen also nicht warten bis zum nächsten Bericht, sondern erhalten Warnhinweise sofort, wenn diese bei einem Audit-Prozess festgestellt wird. Ab dem zweiten Jahr wird dieser Service allerdings kostenpflichtig. Optional können Sie nach jeder Lieferung eines Berichts den Baustein **OSINT Audit** hinzubuchen.

Bitte beachten Sie, dass wir im Zuge der Ergebnisbesprechung der Berichte keine Beratung anbieten können – wir bewerten die Auditergebnisse lediglich im Kontext der Bezugsnorm ISO 27001.

*nach dem CyDIS Scoring

27001OSINT – CYBER SCORING*

Kurzübersicht Produkte:

Produkt	Empfehlung
27001OSINT PRE	Sind möchten ein schnellen und kompakten Einstieg in das Thema Informationssicherheit und ggf. schon reale Bedrohungen erkennen können – dann ist dieser Einstiegsreport der Richtige für Sie! **Zielgruppe: Geschäftsführung, Oberste Leitung**
27001OSINT PRE+	Sie haben sich schon mit dem Thema Informationssicherheit nach ISO 27001 befasst – möchten aber schon detailliert wissen, wie Ihnen ein Managementsystem nach ISO 27001 helfen kann konkrete Schwachstellen zu beseitigen – dann ist dieser Bericht ein guter Einstieg zur Analyse von Schwachstellen in Bezug auf die Anforderungen und Hilfestellungen der ISO 27001. **Zielgruppe: Geschäftsführung, Oberste Leitung, IT-Leitung**
27001OSINT POST	Sie haben bereits ein Managementsystem nach ISO 27001 (ISMS) eingeführt und möchten wissen, welche realen Schwachstellen trotzdem noch aktuell existieren – dann sollten Sie nicht zögern und diesen Report anfordern. Dieser Auditbericht liefert Ihnen Auskunft über die Prozessqualität Ihres ISMS und hilft Ihnen aktuelle Schwachstellen zu erkennen. **Zielgruppe: CISO (ISB), IT-Leitung**
27001OSINT CONT	Sie möchten auf dem Laufenden bleiben, wissen ob Maßnahmen greifen, ob neue Bedrohungen sich auf Ihr Unternehmen ggf. schon auswirken? Dann ist unser Continuity Bericht genau das Richtige – Sie erhalten quartalsweise einen Bericht und ein tägliches Alerting (im ersten Jahr kostenlos) sollten sich aktuelle Werte wesentlich verändern. **Zielgruppe: CISO (ISB), IT-Leitung**
OSINT Audit	Sie möchten den OSINT Audit-Bericht besser verstehen? Wir bieten Ihnen eine Ergebnisbesprechung (keine Beratung!) mit einem erfahrenen Auditor aus unserem Hause an – in der Regel kann er Ihnen die Ergebnisse innerhalb von einem Tag eingehend erläutern. **Zielgruppe: Geschäftsführung, Oberste Leitung, CISO (ISB)**

Preise auf Anfrage...

Sprechen Sie uns an unter: it@dqsbit.de oder 069-95427-8881 – wir informieren Sie gerne!

*nach dem CyDIS Scoring