DAS CYBERRISK RATING

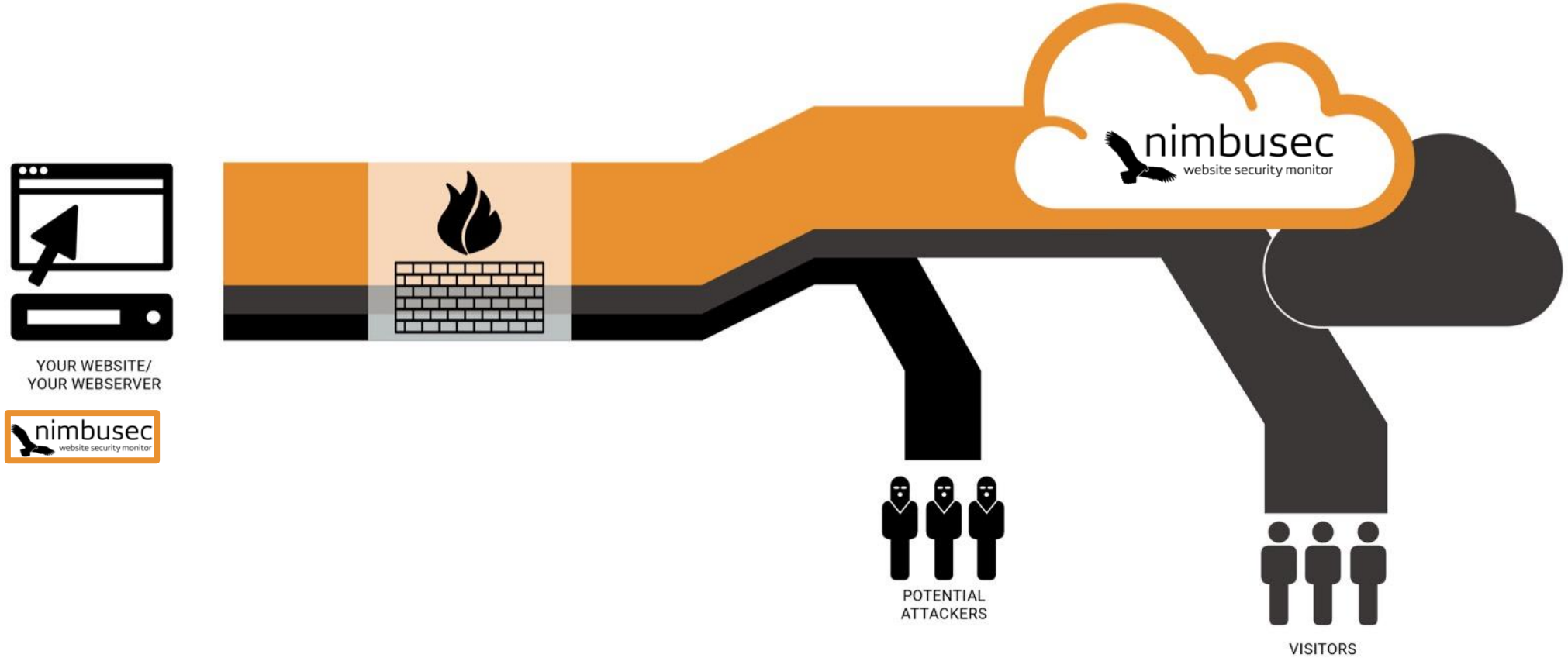
by KSV1870

Mag. Alexander Mitter

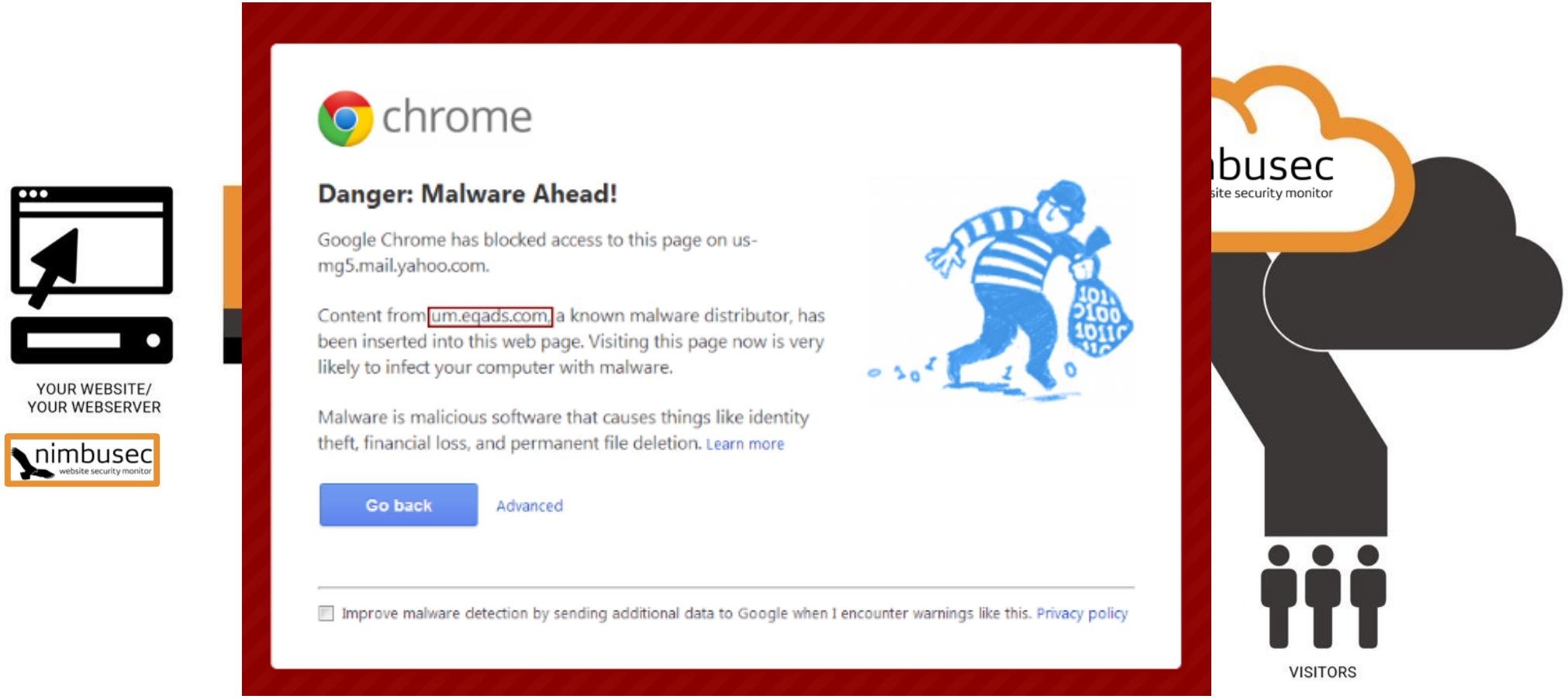
GF KSV1870 Nimbusec

4. E-Commerce Fraud Forum 2022

Wie kann sich ein Onlineshop gegen Hacker wehren und damit das eigene CyberRisk Rating by KSV1870 verbessern?


YOUR WEBSITE/
YOUR WEBSERVER
nimbusec
website security monitor
nimbusec
website security monitor
POTENTIAL
ATTACKERS
VISITORS


Hacked By Pro_Mast3r ~
Attacker Gov
Nothing Is Impossible
Peace From Iraq
YOUR WE
YOUR WEB
nimbu
VISITORS


YOUR WEBSITE/
YOUR WEBSERVER
nimbusec
website security monitor
chrome
Danger: Malware Ahead!
Google Chrome has blocked access to this page on us-mg5.mail.yahoo.com.
Content from um.eqads.com, a known malware distributor, has been inserted into this web page. Visiting this page now is very likely to infect your computer with malware.
Malware is malicious software that causes things like identity theft, financial loss, and permanent file deletion. Learn more
Go back
Advanced
Improve malware detection by sending additional data to Google when I encounter warnings like this. Privacy policy
VISITORS

DAS CYBERRISK RATING by KSV1870

SIGN IN The Register

{* SECURITY *}

British Airways hack: Infosec experts finger third-party scripts on payment pages

Airline yet to reveal breach's cause

John Leyden Tue 11 Sep 2018 // 10:37 UTC

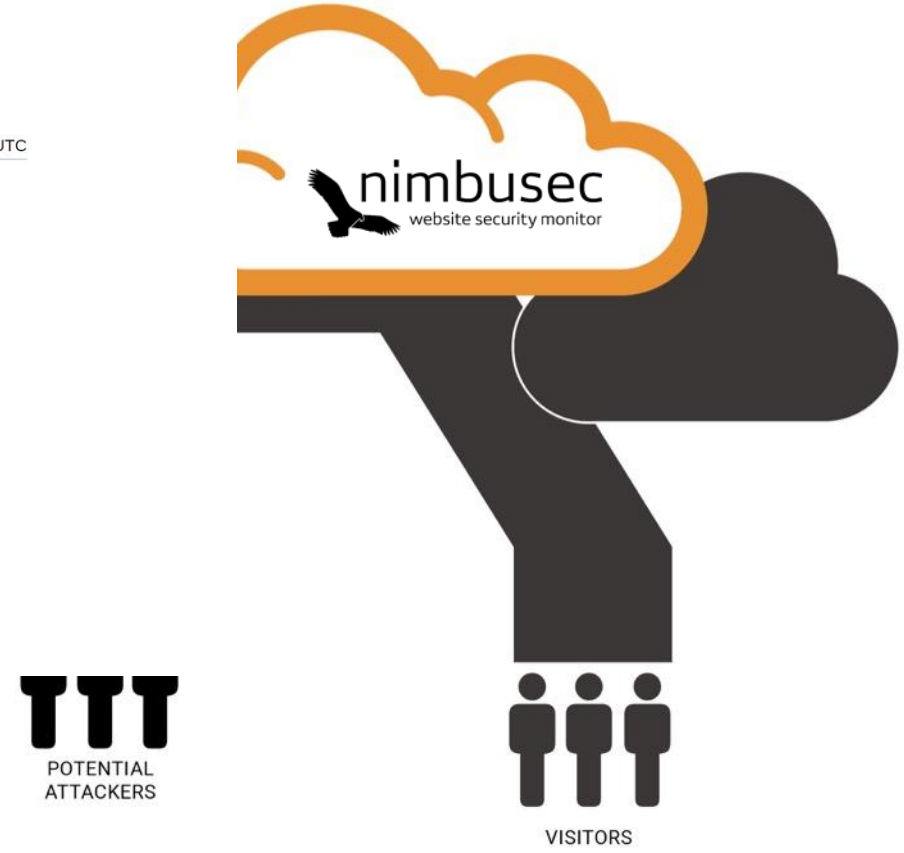
86

Security experts are debating the cause of the British Airways mega-breach, with external scripts on its payment systems emerging as a prime suspect in the hack.

BA has said little related to the cause of the breach, much less who might have carried it out. Security vendor RiskIQ has advanced the theory that malicious code was planted on the airline's payments page, via a modified version of the Modernizr JavaScript library. To carry out the attack in this way, hackers would have had to modify JavaScript files without hobbling its core functionality.

Why infosec folk think it was the payment system

Although BA hasn't disclosed the root of the breach, the unusual precision it ascribed to the hack's duration suggests it may already know what happened.



https://www.theregister.com/2018/09/11/british_airways_website_scripts/

SIGN IN

{* SECURITY *}

British Airways hack: party scripts on paym

Airline yet to reveal breach's cause

John Leyden

86

Security experts are debat with external scripts on its the hack.

BA has said little related tc the breach, much less whc carried it out. Security ven has advanced the theory t code was planted on the a payments page, via a moc of the Modernizr JavaScri carry out the attack in this would have had to modify files without hobbling its cc functionality.

ico. Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Home | Your data matters | For organisations | Make a complaint | Action we've taken | About the ICO

About the ICO / News and events / News and blogs /
ICO fines British Airways £20m for data breach affecting more than 400,000 customers

ICO fines British Airways £20m for data breach affecting more than 400,000 customers

Date **16 October 2020**
Type **News**

The Information Commissioner's Office (ICO) has fined British Airways (BA) £20m for failing to protect the personal and financial details of more than 400,000 of its customers.

An ICO investigation found the airline was processing a significant amount of personal data without adequate security measures in place. This failure broke data protection law and, subsequently, BA was the subject of a cyber-attack during 2018, which it did not detect for more than two months.

ICO investigators found BA ought to have identified weaknesses in its security and resolved them with security measures that were available at the time.

Addressing these security issues would have prevented the 2018 cyber-attack being carried out in this way, investigators concluded.

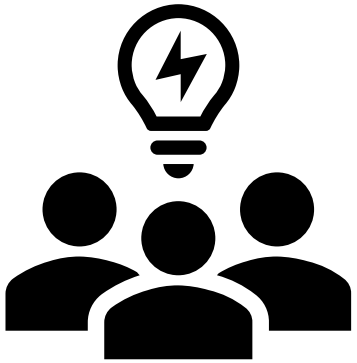
Information Commissioner Elizabeth Denham said: "People entrusted their personal details to BA and BA failed to take adequate measures to keep those details secure.

"Their failure to act was unacceptable and affected hundreds of thousands of people, which may have caused some anxiety and distress as a result. That's why we have

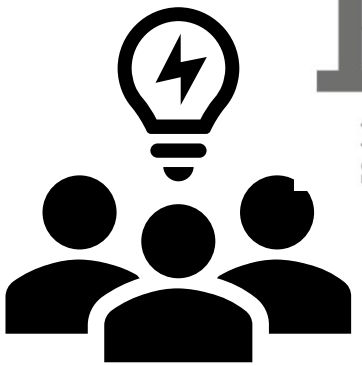
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/

DAS CYBERRISK RATING by KSV1870

Wie kann sich ein Onlineshop gegen Hacker wehren und damit das eigene CyberRisk Rating by KSV1870 verbessern?



DAS CYBERRISK RATING by KSV1870



KSÖ Kompetenzzentrum Sicheres Österreich

Cyber Risk Advisory Board des KSÖ

CISOs der österreichischen Industrie
im Dialog mit der operativen NIS Behörde

DAS CYBERRISK RATING by KSV1870

KSÖ Kompetenzzentrum Sicheres Österreich

Cyber Risk Advisory Board des KSÖ
CISOs der österreichischen Industrie
im Dialog mit der operativen NIS Behörde

beschließt

CRR Schema Policy 202... 12 / 18 80%

CRR Schema Policy

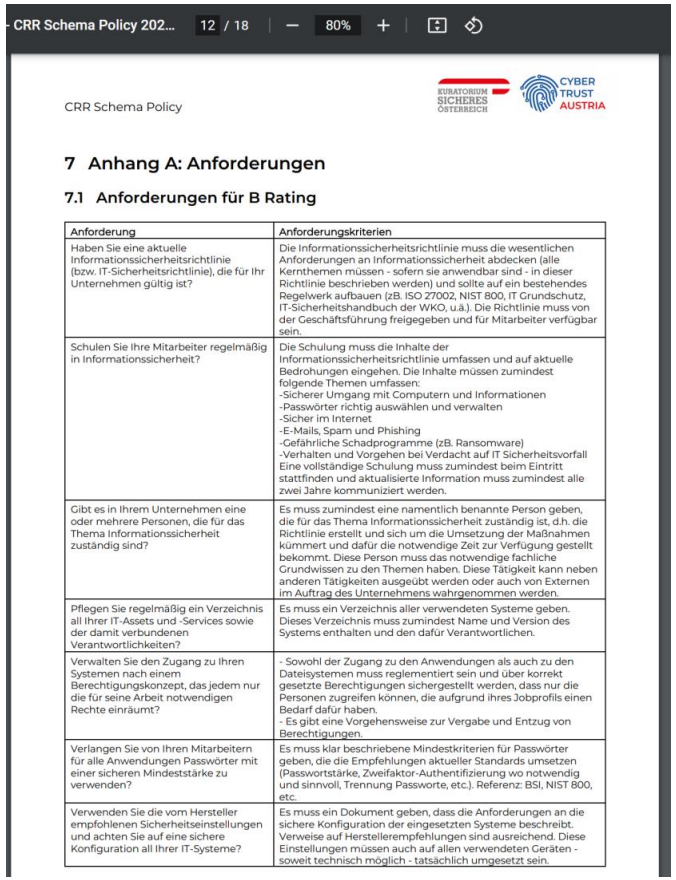
KURATORIUM SICHERES ÖSTERREICH CYBER TRUST AUSTRIA

7 Anhang A: Anforderungen

7.1 Anforderungen für B Rating

Anforderung	Anforderungskriterien
Haben Sie eine aktuelle Informationssicherheitsrichtlinie (bzw. IT-Sicherheitsrichtlinie), die für Ihr Unternehmen gültig ist?	Die Informationssicherheitsrichtlinie muss die wesentlichen Anforderungen an Informationssicherheit abdecken (alle Kernthemen müssen - sofern sie anwendbar sind - in dieser Richtlinie beschrieben werden) und sollte auf ein bestehendes Regelwerk aufbauen (zB. ISO 27002, NIST 800, IT Grundschutz, IT-Sicherheitshandbuch der WKO, u.ä.). Die Richtlinie muss von der Geschäftsführung freigegeben und für Mitarbeiter verfügbar sein.
Schulen Sie Ihre Mitarbeiter regelmäßig in Informationssicherheit?	Die Schulung muss die Inhalte der Informationssicherheitsrichtlinie umfassen und auf aktuelle Bedrohungen eingehen. Die Inhalte müssen zumindest folgende Themen umfassen: -Sicherer Umgang mit Computern und Informationen -Passwörter richtig auswählen und verwalten -Sicher im Internet -E-Mails, Spam und Phishing -Gefährliche Schadprogramme (zB. Ransomware) -Verhalten und Vorgehen bei Verdacht auf IT Sicherheitsvorfall Eine vollständige Schulung muss zumindest beim Eintritt stattfinden und aktualisierte Information muss zumindest alle zwei Jahre kommuniziert werden.
Gibt es in Ihrem Unternehmen eine oder mehrere Personen, die für das Thema Informationssicherheit zuständig sind?	Es muss zumindest eine namentlich benannte Person geben, die für das Thema Informationssicherheit zuständig ist, d.h. die Richtlinie erstellt und sich um die Umsetzung der Maßnahmen kümmert und dafür die notwendige Zeit zur Verfügung gestellt bekommt. Diese Person muss das notwendige fachliche Grundwissen zu den Themen haben. Diese Tätigkeit kann neben anderen Tätigkeiten ausgeübt werden oder auch von Externen im Auftrag des Unternehmens wahrgenommen werden.
Pflegen Sie regelmäßig ein Verzeichnis all Ihrer IT-Assets und -Services sowie der damit verbundenen Verantwortlichkeiten?	Es muss ein Verzeichnis aller verwendeten Systeme geben. Dieses Verzeichnis muss zumindest Name und Version des Systems enthalten und den dafür Verantwortlichen.
Verwalten Sie den Zugang zu Ihren Systemen nach einem Berechtigungskonzept, das jedem nur die für seine Arbeit notwendigen Rechte einräumt?	- Sowohl der Zugang zu den Anwendungen als auch zu den Dateisystemen muss reglementiert sein und über korrekt gesetzte Berechtigungen sichergestellt werden, dass nur die Personen zugreifen können, die aufgrund ihres Jobprofils einen Bedarf dafür haben. - Es gibt eine Vorgehensweise zur Vergabe und Entzug von Berechtigungen.
Verlangen Sie von Ihren Mitarbeitern für alle Anwendungen Passwörter mit einer sicheren Mindeststärke zu verwenden?	Es muss klar beschriebene Mindestkriterien für Passwörter geben, die die Empfehlungen aktueller Standards umsetzen (Passwortstärke, Zweifaktor-Authentifizierung wo notwendig und sinnvoll, Trennung Passworte, etc.). Referenz: BSI, NIST 800, etc.
Verwenden Sie die vom Hersteller empfohlenen Sicherheitseinstellungen und achten Sie auf eine sichere Konfiguration all Ihrer IT-Systeme?	Es muss ein Dokument geben, dass die Anforderungen an die sichere Konfiguration der eingesetzten Systeme beschreibt. Verweise auf Herstellerempfehlungen sind ausreichend. Diese Einstellungen müssen auch auf allen verwendeten Geräten - soweit technisch möglich - tatsächlich umgesetzt sein.

Das CyberRisk Rating by KSV1870



CRR Schema Policy 202... 12 / 18 80%

CRR Schema Policy

KURATORIUM SICHERES ÖSTERREICH

CYBER TRUST AUSTRIA

7 Anhang A: Anforderungen

7.1 Anforderungen für B Rating

Anforderung	Anforderungskriterien
Haben Sie eine aktuelle Informationssicherheitsrichtlinie (bzw. IT-Sicherheitsrichtlinie), die für Ihr Unternehmen gültig ist?	Die Informationssicherheitsrichtlinie muss die wesentlichen Anforderungen an Informationssicherheit abdecken (alle Kernthemen müssen - sofern sie anwendbar sind - in dieser Richtlinie beschrieben werden) und sollte auf ein bestehendes Regelwerk aufbauen (zB. ISO 27002, NIST 800, IT Grundschutz, IT-Sicherheitshandbuch der WKO, u.ä.). Die Richtlinie muss von der Geschäftsführung freigegeben und für Mitarbeiter verfügbar sein.
Schulen Sie Ihre Mitarbeiter regelmäßig in Informationssicherheit?	Die Schulung muss die Inhalte der Informationssicherheitsrichtlinie umfassen und auf aktuelle Bedrohungen eingehen. Die Inhalte müssen zumindest folgende Themen umfassen: -Sicherer Umgang mit Computern und Informationen -Passwörter richtig auswählen und verwalten -Sicher im Internet -E-Mails, Spam und Phishing -Gefährliche Schadprogramme (zB. Ransomware) -Verhalten und Vorgehen bei Verdacht auf IT Sicherheitsvorfall Eine vollständige Schulung muss zumindest beim Eintritt stattfinden und aktualisierte Information muss zumindest alle zwei Jahre kommuniziert werden.
Gibt es in Ihrem Unternehmen eine oder mehrere Personen, die für das Thema Informationssicherheit zuständig sind?	Es muss zumindest eine namentlich benannte Person geben, die für das Thema Informationssicherheit zuständig ist, d.h. die Richtlinie erstellt und sich um die Umsetzung der Maßnahmen kümmert und dafür die notwendige Zeit zur Verfügung gestellt bekommt. Diese Person muss das notwendige fachliche Grundwissen zu den Themen haben. Diese Tätigkeit kann neben anderen Tätigkeiten ausgeübt werden oder auch von Externen im Auftrag des Unternehmens wahrgenommen werden.
Pflegen Sie regelmäßig ein Verzeichnis all Ihrer IT-Assets und -Services sowie der damit verbundenen Verantwortlichkeiten?	Es muss ein Verzeichnis aller verwendeten Systeme geben. Dieses Verzeichnis muss zumindest Name und Version des Systems enthalten und den dafür Verantwortlichen.
Verwalten Sie den Zugang zu Ihren Systemen nach einem Berechtigungskonzept, das jedem nur die für seine Arbeit notwendigen Rechte einräumt?	- Sowohl der Zugang zu den Anwendungen als auch zu den Dateisystemen muss reglementiert sein und über korrekt gesetzte Berechtigungen sichergestellt werden, dass nur die Personen zugreifen können, die aufgrund ihres Jobprofils einen Bedarf dafür haben. - Es gibt eine Vorgehensweise zur Vergabe und Entzug von Berechtigungen.
Verlangen Sie von Ihren Mitarbeitern für alle Anwendungen Passwörter mit einer sicheren Mindeststärke zu verwenden?	Es muss klar beschriebene Mindestkriterien für Passwörter geben, die die Empfehlungen aktueller Standards umsetzen (Passwortstärke, Zweifaktor-Authentifizierung wo notwendig und sinnvoll, Trennung Passworte, etc.). Referenz: BSI, NIST 800, etc.
Verwenden Sie die vom Hersteller empfohlenen Sicherheitseinstellungen und achten Sie auf eine sichere Konfiguration all Ihrer IT-Systeme?	Es muss ein Dokument geben, dass die Anforderungen an die sichere Konfiguration der eingesetzten Systeme beschreibt. Verweise auf Herstelleremfehlungen sind ausreichend. Diese Einstellungen müssen auch auf allen verwendeten Geräten - soweit technisch möglich - tatsächlich umgesetzt sein.

bestimmt

CYBERRISK RATING

ENGLISH KONTAKT

FÜR KRITISCHE INFRASTRUKTUR & ENTERPRISE FÜR BEWERTETE UNTERNEHMEN

DIGITALE RISIKEN IN LIEFERKETTEN SICHTBAR MACHEN

DIE GESAMTLÖSUNG FÜR THIRD PARTY CYBER-RISK MANAGEMENT ENTSPRECHEND NIS & DSGVO – WELTWEIT EINSETZBAR.

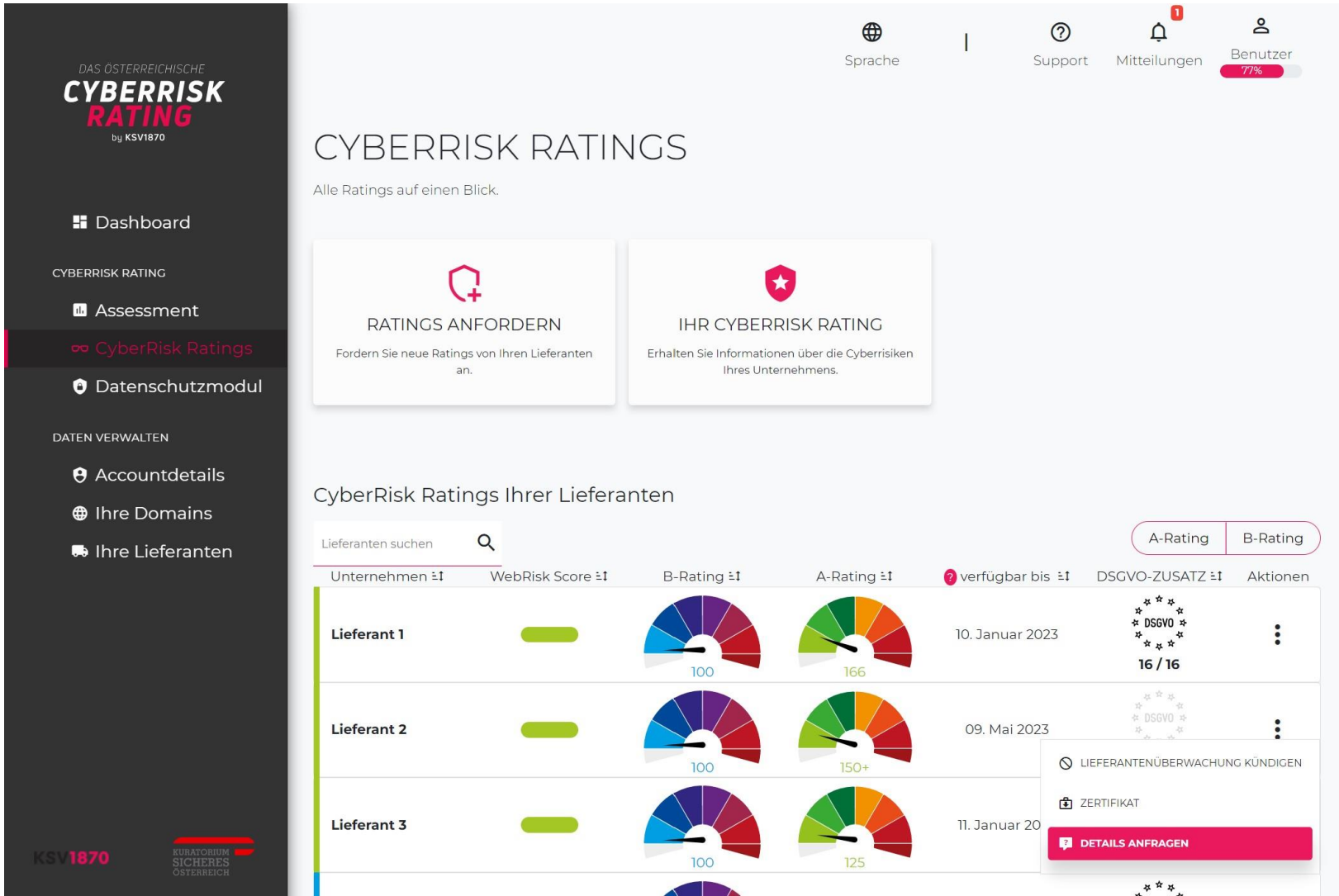
Bewertung von IT-Security, DSGVO-Compliance & Business Continuity Management leicht gemacht – mit dem CyberRisk Rating by KSV1870 .

WIE KÖNNEN WIR IHNEN HELFEN?

Das CyberRisk Rating by KSV1870 erfüllt laut der österreichischen operativen NIS-Behörde (BMI) die Anforderungen des NIS-Gesetzes für Lieferantenrisiken (§ 11 Abs. 1 Z 2 iVm Anlage 1 NISV).

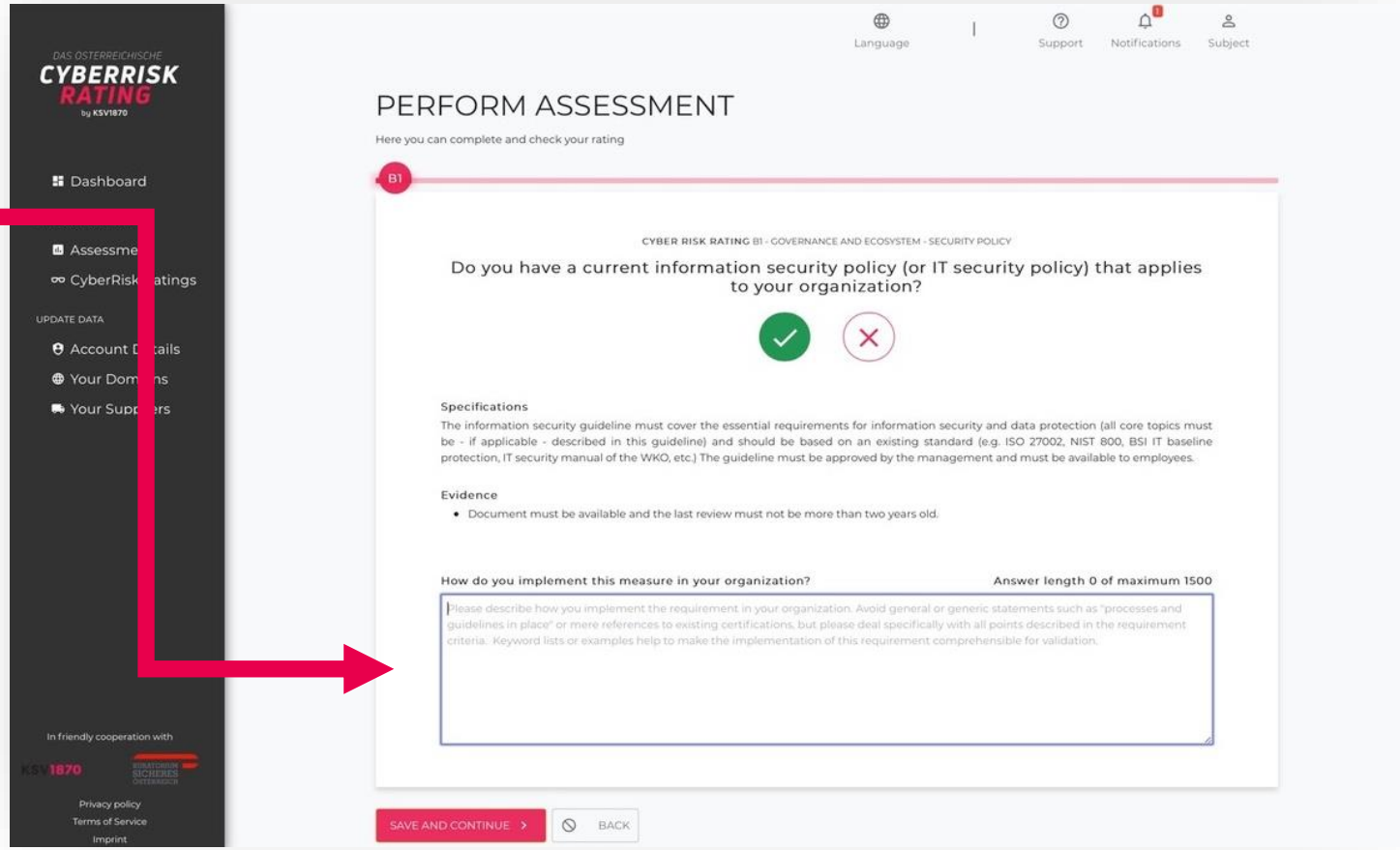
Mehr Informationen finden Sie unter https://www.nis.gv.at/.

Das CyberRisk Rating by KSV1870



Ein einfaches „Ja“ reicht nicht aus.
Die Validierung.

- Prozess auf **Deutsch und Englisch**
- Eine **„Ja“** Antwort erfordert die **Beschreibung** der **Anforderungserfüllung** in eigenen Worten.
- Damit wird **korrektes Verständnis** und **ausreichende Umsetzung** überprüft.
- Die Antworten müssen **objektiv nachvollziehbar** sein. Nur dann verbessert sich das Rating.



DAS CYBERRISK RATING by KSV1870

Warum können Sie dem Rating vertrauen?

Informationen direkt vom bewerteten Unternehmen. Geprüft. Fair.

- Validierung des ausgefüllten Assessments durch IT-Spezialisten

VALIDIERUNG

1

2

KORREKTUR

- Nach der Validierung hat das bewertete Unternehmen die Möglichkeit, unklare Antworten zu korrigieren

- Korrigierte Antworten werden nun endgültig verifiziert

VERIFIZIERUNG

3

4

AUDIT

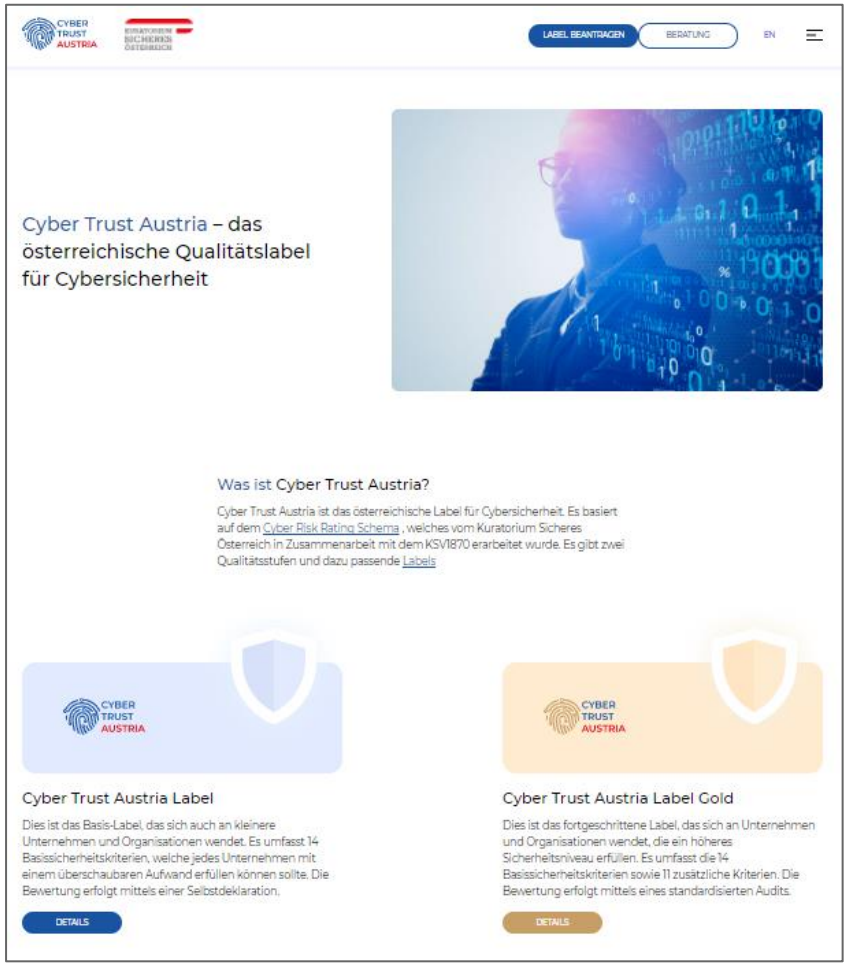
- **Audit aller Angaben möglich!**
- Zusammenarbeit mit „Qualifizierten Stellen“ des BMI

Kann ich mit IT-Sicherheit werben?
CyberTrust Label als Qualitätskriterium

- Das CyberTrust Label steht allen Organisationen offen, die ein ausgezeichnetes Rating unter 190 erzielen (zur Referenz: Minimales Risiko=100, Höchstes Risiko=700).

- **Ein Lieferant, der ein CyberTrust Label besitzt, wird kostenlos im KSV1870 CyberRisk Rating Portal aufgeführt und hat damit einen Wettbewerbsvorteil.**

- Die Kosten einer CyberTrust Label Prüfung liegen bei 890€ exkl. USt. und sind damit auch für KMU erreichbar.



Quelle: https://www.cyber-trust.at/

Zusammenfassung

Wie gegen Hacker wehren und damit das CyberRisk-Rating verbessern?

1. **Nutzen Sie das Wissen der Experten:**
   - https://cyberrisk-rating.at/CyberRisk-Rating_Anforderungen_V2_DEUTSCH.pdf

2. **Testen Sie, wo Ihr Unternehmen steht:**
   - https://demo.cyberrisk-rating.at/

3. **Werben Sie mit Ihrer guten Vorbereitung:**
   - https://www.cyber-trust.at/

DAS CYBERRISK RATING by KSV1870

Ihr Ansprechpartner:

Alexander Mitter
CEO KSV1870 Nimbusec

a.mitter@nimbusec.com
+43 732 860 626 (Büro)
+43 699 144 155 11 (direkt)