netscan24

REPORT
XY UNTERNEHMEN GMBH

vom XX. Monatsname XXXX

ANALYSEDATUM

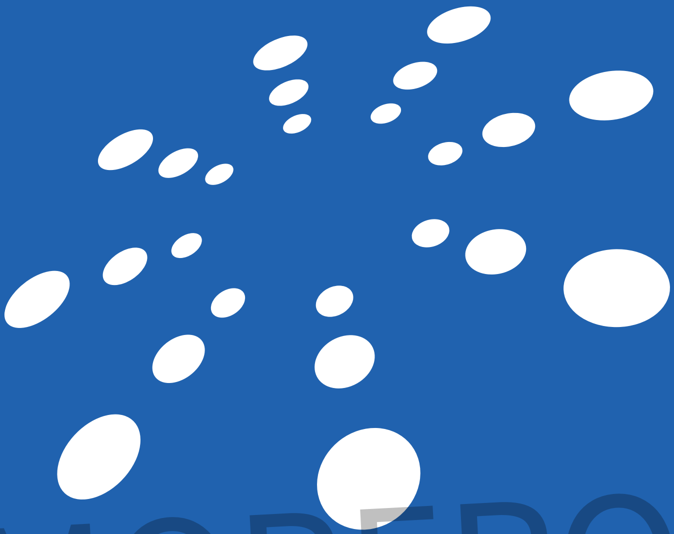
vom XX. Monatsname XXXX bis zum XX. Monatsname XXXX

INHALTSVERZEICHNIS IP 172.217.22.35

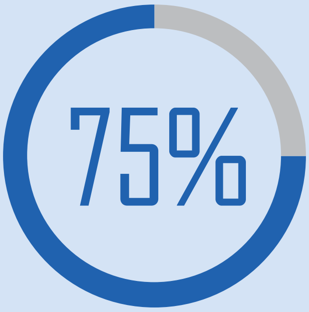
Management Summery

Technical Details

REPORT FÜR GESCHÄFTSFÜHRER



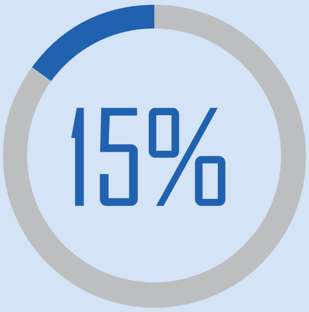
MANAGEMENT SUMMERY



HOCH KRITISCHE SCHWACHSTELLEN

Sie sollten sich schnellsten diesen Problemen widmen.

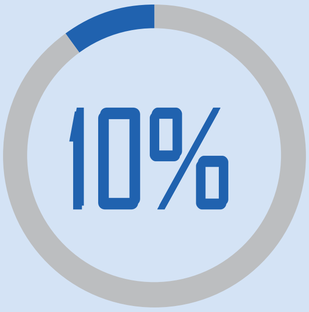
75 Probleme sollten behoben werden



KRITISCHE SCHWACHSTELLEN

Sie sollten sich in der nächsten Zeit diesen Problemen widmen.

15 Probleme sollten behoben werden

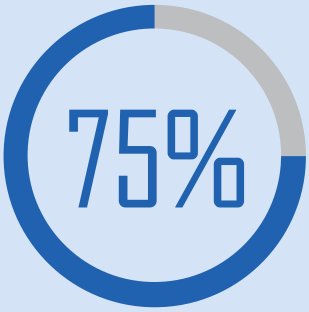


SCHWACHSTELLEN

Sie sollten sich in der nächsten Zeit diesen Problemen widmen.

10 Probleme sollten behoben werden

MANAGEMENT SUMMERY / HOCHKRITISCHE SCHWACHSTELLEN



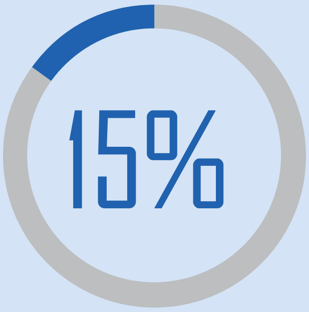
HOCHKRITISCHE SCHWACHSTELLEN

Sie sollten sich dringend um diese Probleme kümmern.

75 Probleme sollten behoben werden

NUMMER	PROBLEM
1	Check for SSL Weak Ciphers
2	SSL Certificate Signed Using A Weak Signature Algorithm

MANAGEMENT SUMMERY / KRITISCHE SCHWACHSTELLEN



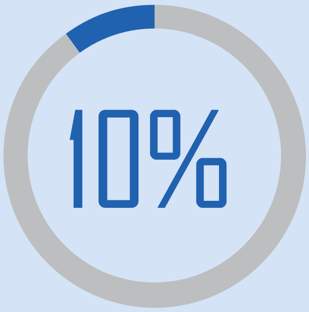
KRITISCHE SCHWACHSTELLEN ⚠

Sie sollten sich in der nächsten Zeit diesen Problemen widmen.

15 Probleme sollten behoben werden

NUMMER	PROBLEM
1	TCP timestamps

MANAGEMENT SUMMERY / SCHWACHSTELLEN



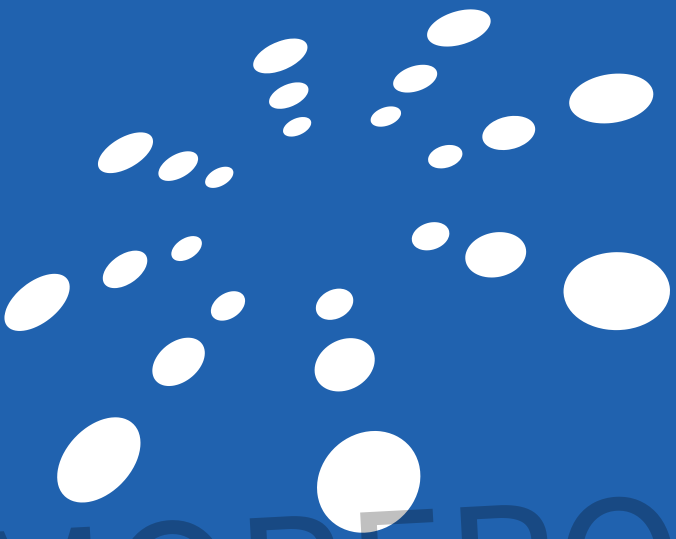
SCHWACHSTELLEN

Sie sollten sich in der nächsten Zeit um diese Probleme kümmern

10 Probleme sollten behoben werden

NUMMER	PROBLEM
1	Check for SSL Weak Ciphers
2	SSL Certificate Signed Using A Weak Signature Algorithm

TECHNISCHER REPORT



TECHNISCHE DETAILS / HOCHKRITISCHE SCHWACHSTELLEN

NAME

SSL Certificate Signed Using A Weak Signature Algorithm

ZUSAMMENFASSUNG

The remote service is using a SSL certificate chain that has been signed using a cryptographically weak hashing algorithm.

ERKLÄRUNG

Secure Hash Algorithm 1 (SHA-1) is considered cryptographically weak and not secure enough for ongoing use. Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when users visit web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates. Servers that use SSL certificates signed using an SHA-1 signature will need to obtain new SHA-2 signed SSL certificates to avoid these web browser SSL certificate warnings.

BESCHREIBUNG

The following certificates are part of the certificate chain but using insecure signature algorithms:
Subject: CN=GeoTrust Global CA,O=GeoTrust Inc.,C=US
Signature Algorithm: sha1WithRSAEncryption

LÖSUNG

The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

BESCHREIBUNG

Weak ciphers offered by this service:
TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA

TECHNISCHE DETAILS / HOCHKRITISCHE SCHWACHSTELLEN

NAME

Check for SSL Weak Ciphers

ZUSAMMENFASSUNG

This routine search for weak SSL ciphers offered by a service.

ERKLÄRUNG

These rules are applied for the evaluation of the cryptographic strength: - Any SSL/TLS using no cipher is considered weak. - All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol. - RC4 is considered to be weak. - 64-bit block cipher 3DES vulnerable to SWEET32 attack(CVE-2016-2183). - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak. - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - CBC ciphers in TLS < 1.2 are considered to be vulnerable to the BEAST or Lucky 13 attacks - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong.

LÖSUNG

The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

BESCHREIBUNG

Weak ciphers offered by this service:

TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA