Rödl & Partner

DIE TÜR IST ZU. DIE FENSTER SIND OFFEN?!

Cybersecurity Risiken aktiv überwachen und bewältigen

„Über das Internet – neu-deutsch Cyberspace – erfolgen mehr und mehr Interaktionen zwischen Geschäftspartnern. Jedes Unternehmen hinterlässt dabei Spuren. Die Notwendigkeit der Unternehmensleitung zur Beurteilung der eigenen Cybersecurity steigt genauso wie die Bedrohungen, denen das Unternehmen aus dem Cyberspace ausgesetzt ist.“

Ein Cybersecurity-Rating kann allen helfen, die Sicherheitsschwächen des eigenen Unternehmens zu erkennen, um entsprechende Gegenmaßnahmen ergreifen zu können.

Aber nicht nur das. Auch die Resilienz wesentlicher Kooperationspartner, Lieferanten und Dienstleister kann mithilfe des Ratings beurteilt werden, da es sich ausschließlich aus Quellen verfügbarer Daten und öffentlicher Informationen aus dem Internet bedient.

SCHWÄCHEN AKTUELLER METHODEN

Die Daten und Informationen der herkömmlichen Instrumente wie Penetrationstests, IDS/IPS, ISMS und spezialisierte IT-Audits haben Schwachstellen:

- Erste Schwachstelle: Sie beziehen nur einen Bruchteil des „Cyberspace" in die Betrachtung mit ein!
- Zweite Schwachstelle: Sie bewerten den Sicherheitsstatus meist nur zu einem bestimmten Zeitpunkt oder Stichtag und liegen damit nicht kontinuierlich vor!

Meist wird dabei die Sicherheit des eigenen Unternehmens bzw. sogar nur der eigenen IT untersucht und bewertet. Das ist nachvollziehbar, ist dies doch der Bereich, den Sie selbst verantworten und auf den Sie Einfluss haben.

DAS CYBERSECURITY-ÖKOSYSTEM

Stellt man sich aber die Frage, mit wem sich das Unternehmen in digitalem Austausch befindet und wer bei digitalen Geschäftsprozessen eine Rolle spielt, dann weitet sich der Blick auf ein sehr komplexes Ökosystem aus.

Dieses komplexe Ökosystem ist für Ihr Unternehmen kritisch und muss berücksichtigt und bewertet werden und das ohne Eingriffe von außen!

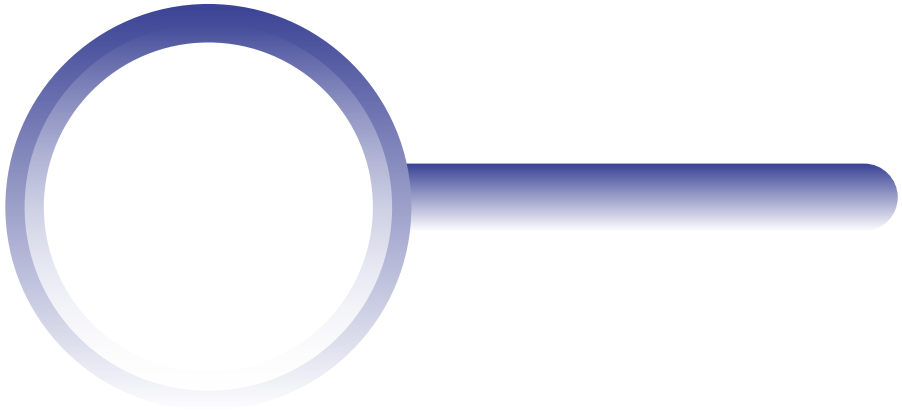
OHNE EINGRIFFE VON AUSSEN!

Ohne Eingriffe von außen? Wie soll das gehen? Ebenso wie jeder Anwender, der durch die Nutzung von Diensten und Services Spuren im Netz hinterlässt, ist auch ein Unternehmen mit seinen Endgeräten und Servern im Netz nicht unbekannt.

KONTI-NUIERLICHE BEURTEILUNG DER CYBER-SICHERHEIT

Mit einem Cybersecurity-Rating bewegen Sie Ihr Unternehmen einen wesentlichen Schritt näher in Richtung eines angemessenen Schutzniveau.

- Sie erhalten als Unternehmensleitung konkrete Hinweise auf technischen und organisatorischen Verbesserungsbedarf Ihrer Systemumgebung und senken somit das Risiko, Opfer von Angriffen zu werden.
- Sie weisen mit den Reports nach, dass Sie steuernd auf die Schutzbedarfe Ihres Unternehmens eingehen und können sich aktiv in die Umsetzung auf IT-Ebene einbringen.
- Sie schützen sich selbst vor Haftungsfragen im Umfeld von Cyberrisiken, da Sie mit dem Rating ein schlüssiges Managementsystem etablieren können, auf dessen Basis bedarfs- und risikoorientiert IT-Sicherheitsmaßnahmen implementiert werden.



VERSCHAFFEN SIE SICH SICHERHEIT!

Unser Cybersecurity-Rating bewertet unterschiedliche Sicherheitsbereiche, von der Botnet Infektion, über das Anwenderverhalten bis hin zum Sicherheitsstatus von mobiler Software.

Es ist z. B. erkennbar, ob Endgeräte oder Server aus dem eigenen Unternehmen mit bekannten Botnetzen kommunizieren oder als gefährlich einzustufende Server (Tauschserver, etc.) außerhalb des eigenen Unternehmens genutzt werden.

AUSFÜHRLICHER BERICHT FÜR IT UND MANAGEMENT

Die Ergebnisse werden in einem Bericht mit einer Management Übersicht und technischen Details zu den einzelnen Sicherheitsbereichen zielgruppengerecht dargestellt.

Ein Beispiel-Bericht

COMPROMISED-SYSTEMS

Botnet Infections	F
Spam Propagation	B
Malware servers	A
Unsolicited communication	A
Potentially Exploited	D

USER BEHAVIOR

File Sharing	C

PUBLIC DISCLOSURES

Breaches	A

DILIGENCE

A	SPF Domains
B	DKIM Records
A	TLS/SSL Certificates
C	TLS/SSL Configurations
C	Open Ports
C	Web Application Headers
B	Patching Cadence
B	Insecure Systems
A	Server Software
D	Desktop Software
D	Mobile Software

SCHNELL UND EFFEKTIV!

Als kritischer Erfolgsbegleiter sehen wir uns als Unterstützer, Ihnen in diesem Umfeld ein Instrument an die Hand zu geben, dass Ihnen Sicherheit gibt. Dabei unterstützen wir Sie mit dem eigentlichen Rating-Report, um die eigene Resilienz oder die Ihrer Dienstleister beurteilen zu können. Wir helfen Ihnen aber auch, bestehende Sicherheitsmaßnahmen zu verbessern und das Rating als ständiges Steuerungsinstrument zu etablieren.

Für das Cybersecurity Rating lassen sich folgende Anwendungsfelder identifizieren:

- Erstellung eines unternehmensspezifischen Cybersecurity Rating Reports und Klärung des Ergebnisses
- Erstellung von Cybersecurity Ratings bei Auftragsdatenverarbeitern im Umfeld des Datenschutzes
- Unterstützung bei der Integration des Instruments in ein vorhandenes ISMS (z. B. ISO / IEC 27001 oder ISIS12)
- Integration des Ratings in die Konzernsteuerung

ANSPRECH-PARTNER

Hannes Hahn

CISA - CSP - DSB, IT-Auditor IDW,
Zert. ISIS12®-Berater

T +49 221 949 909 165
E hannes.hahn@roedl.com

Falk Hofmann

Dipl.-Ing. Elektrotechnik,
IT-Auditor, ISO27001 Auditor, DSB

T +49 30 81 079 584
E falk.hofmann@roedl.com

Rödl IT Secure GmbH
Äußere Sulzbacher Straße 100
90491 Nürnberg

T +49 221 949 909 0
E cybersecurity@roedl.com

www.roedl.de