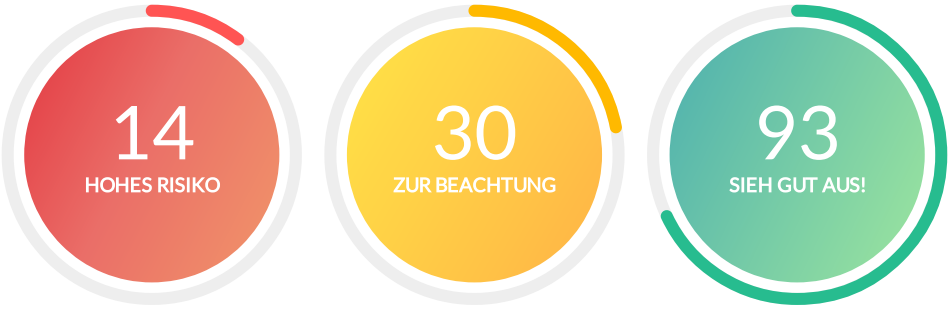
KYND START

Cyber-Risikofaktoren



Ransomware

KYND hat die öffentlich zugängliche Internetinfrastruktur der Organisation überprüft, um ihre Anfälligkeit für einen Ransomware-Angriff zu bewerten.

Example ist in Gefahr!

E-Mail-Sicherheit

KYND hat die SPF- und DMARC-Richtlinien der Organisation überprüft und diese Richtlinien auf ihre Anfälligkeit für E-Mail-Spoofing bewertet.

@example.com E-Mails können gefälscht werden!

-gegen- andere ähnlich Organisationen

wo Unternehmen im Rennen um Cybersicherheit steht

Zertifikatsprobleme

20% Ihrer Zertifikate sind veraltet oder nicht vertrauenswürdig

Sicherheitszertifikate auf Ihren Websites schützen Nutzerdaten und bestätigen die Site-Authentizität. Bei Verwendung veralteter oder unzuverlässiger Zertifikate erhalten Besucher Browserwarnungen und Anwendungen können versagen. Stellen Sie sicher, dass Sie Ihre Zertifikate pflegen, erneuern oder nicht benötigte entfernen.

Hinterherhinkend	Zurückgefallen	In der Gruppe
	✓	

Falsch konfigurierte Dienste

8% Ihrer Dienste sind falsch konfiguriert

Nicht alle Teile Ihrer IT-Infrastruktur müssen öffentlich zugänglich sein. Datenbanken, Admin-Panels und Entwicklerzugänge sollten nur intern verfügbar sein, um Angriffe zu verhindern. Beschränken Sie den Zugriff auf notwendige Personen.

Hinterherhinkend	Zurückgefallen	In der Gruppe
✓		

Veraltete Dienste

8% Ihrer Dienste sind erheblich veraltet

Halten Sie Ihre Dienste aktuell, um Ihre Online-Sicherheit zu gewährleisten. Veraltete Versionen enthalten oft bekannte Schwachstellen, die von Hackern ausgenutzt werden können. Durch Updates auf die neueste Version schützen Sie Ihre Dienste vor solchen Risiken.

Hinterherhinkend	Zurückgefallen	In der Gruppe
		✓

Domain-Schutz

0% Ihrer Domains haben Probleme

Der Verlust der Kontrolle über Ihre Domains birgt ein Geschäftsrisiko. Werden Domains auf persönliche E-Mail-Adressen oder Agenturen registriert, können wichtige Updates und Fristen verpasst werden und Hacker haben es leichter, die Kontrolle zu übernehmen.

Hinterherhinkend	Zurückgefallen	In der Gruppe
		✓

KYND START

Wo soll ich anfangen...

KYND empfiehlt, diese Punkte zuerst zu überprüfen, um Ihre nächsten Schritte zu priorisieren.

1 Schließen Sie den offenen RDP-Zugang zu Ihrer Infrastruktur

Es gibt 2 Remote Desktop Protocol (RDP)-Dienste, die öffentlich zugänglich sind. RDP wird häufig ausgenutzt, um Ransomware zu verbreiten und Daten zu stehlen, was die Organisation für diese Arten von Angriffen anfällig macht.

RDP-Dienste sollten hinter Firewalls geschützt und auf interne Netzwerke beschränkt werden. Darüber hinaus sollte der RDP-Zugang nur den Systemen und Konten der Organisation gewährt werden, wo dies unbedingt erforderlich ist, und in diesen begrenzten Fällen sollte eine Multi-Faktor-Authentifizierung (MFA) erforderlich sein.

Risikofaktoren

- Verwundbare Vermögenswerte
- Ransomware
- Schadsoftware
- Unterbrechung des Geschäftsbetriebs

2 Aktualisieren Sie verwundbare Software

Es gibt 3 anfällige Instanzen von Microsoft IIS in der Infrastruktur der Organisation, die ein Risiko für Malware und Ransomware darstellen

Microsoft IIS-Version 7.5 ist veraltet und muss dringend gepatcht werden

Aktualisieren Sie Microsoft IIS und Windows Server auf die neueste Version

Risikofaktoren

- Verwundbare Vermögenswerte
- Ransomware
- Schadsoftware
- Unterbrechung des Geschäftsbetriebs

3 Öffentlichen Zugriff auf Datenbankservices schließen

Es gibt 2 Datenbanken, die öffentlich zugänglich sind und anderen die Kontrolle über Vermögenswerte ermöglichen oder die Installation von Ransomware erlauben. Selbst wenn diese Datenbanken durch Passwörter geschützt sind, ermöglicht der offene Zugang Angreifern, ihre Angriffe leicht zu starten und Zugang zu diesen Systemen zu erhalten.

Datenbanken sollten durch Firewalls geschützt und auf interne Netzwerke beschränkt werden, um zu verhindern, dass Angreifer Zugriff auf interne und Kundendaten der Organisation erhalten

Risikofaktoren

- Öffentliche/unbesicherte Vermögenswerte
- Datendiebstahl
- Ransomware
- Sicherheit

4 Fügen Sie eine E-Mail-Spoofing-Richtlinie hinzu

Es gibt keinen DMARC Eintrag für @example.com E-Mails, was sie anfällig für Spoofing macht. Selbst wenn Sie einen Schutz für eingehende Mails haben, verhindert dies nicht, dass externe Empfänger (wie Kunden, Lieferanten und andere wichtige Geschäftskontakte) E-Mails erhalten, die @example.com imitieren.
Ein grundlegender DMARC-Eintrag sollte hinzugefügt werden, um das Monitoring von gefälschten E-Mails zu beginnen.

Fügen Sie dies als txt-Datensatz auf _dmarc.example.com hinzu:

„v=DMARC1; p=none; rua=mailto:[insertAddress]@example.com“

Risikofaktoren

- Phishing
- E-Mail
- Finanziell
- Ruf

5 Aktualisieren Sie veraltete Software

1 Veraltete Dienste in der Infrastruktur der Organisation bergen das Risiko von Malware und Ransomware

Diese Dienste sind veraltet und werden nicht mehr unterstützt.

Aktualisieren Sie veraltete Dienste auf eine unterstützte Version, um die neuesten Sicherheitspatches zu erhalten

Risikofaktoren

- Verwundbare Vermögenswerte
- Ransomware
- Schadsoftware
- Unterbrechung des Geschäftsbetriebs

KYND START

Bericht für Unternehmen

Wie KYND Ihre Ergebnisse ermittelt

Startpunkt

Wir haben example.com und 4 andere Domains als Ausgangspunkt für die Organisation verwendet

Entdeckung

Von diesem Ausgangspunkt aus suchten wir nach anderen Domains, die unserer Meinung nach mit der Organisation verbunden sind.

Scannen

Wir haben Subdomains, IPs, E-Mail-Einstellungen und andere mit diesen Domains verbundene Assets gescannt

Bewertung

Wir haben die Ergebnisse unserer Scans bewertet, um die relevanten Risiken für die Organisation zu identifizieren.

Hohe Risiken

Dies sind die Probleme, die KYND als aktive Risiken für Ihre Organisation identifiziert hat. Wenn diese erfolgreich von Angreifern ausgenutzt werden, schaden sie dem Unternehmen auf eine von mehreren Arten: Datenverlust, finanzieller Verlust, Unterbrechung des Geschäftsbetriebs, regulatorische Konsequenzen oder Rufschädigung.

#1 Verwundbare Dienste

- Öffentliche/unbesicherte Vermögenswerte
- Kontrolle von Vermögenswerten
- Ransomware
- Sicherheit

example.com: Remote Desktop Protocol remote_desktop verwendet derzeit den Port 3389 auf der IP-Adresse xxx und ist direkt sichtbar und zugänglich vom Internet aus. Bestimmte Ports (Verbindungen), die direkt sichtbar und zugänglich vom Internet aus sind, stellen ein erhebliches Risiko dar, da sie von Hackern ausgenutzt werden können, um Zugang zu erlangen. Dieser Port sollte sofort hinter einer Firewall versteckt oder der Port geschlossen werden.

#2 Ende des Servicelebens

- Verwundbare Vermögenswerte
- Unterbrechung des Geschäftsbetriebs
- Schadsoftware
- Ransomware

3 Ihrer Organisation laufen auf einer Version von Windows Server 2008, die am 14. Januar 2020 das 'Ende des Lebenszyklus' erreicht hat. Diese Version von Windows Server wird vom Hersteller nicht mehr unterstützt. Neu entdeckte Sicherheitslücken werden nicht mehr behoben und können gezielt von Hackern ausgenutzt werden. Ohne Produktsupport ist eine Organisation, die diesen Server nach diesem Datum weiter betreibt, extrem anfällig für Angriffe und Dienstausfälle.

Diese 3 website Dienste sollten auf ihre neueste Version aktualisiert werden. Da sie mit der Version des Betriebssystems verknüpft sind, ist es wahrscheinlich, dass das gesamte System auf eine neue Version von Windows aktualisiert werden muss.

Weitere Details finden Sie auf der Microsoft-Website oder lesen Sie unseren Blog-Post für weitere Informationen: https://www.kynd.io/windows-server-2008-end-of-life/

Die betroffenen Dienste finden Sie unter:
- Port 443 auf IP-Adresse xxx (zugänglich über example.com)
- Port 443 auf IP-Adresse xxx (zugänglich über example..com)
- Port 80 auf IP-Adresse xxx (zugänglich über example.com)

#3 Veraltete Software

- Verwundbare Vermögenswerte
- Unterbrechung des Geschäftsbetriebs
- Schadsoftware
- Ransomware

example.com: PPTP n/a wird nicht mehr von seinem Entwickler unterstützt. Veraltete Dienste werden nicht mehr unterstützt oder gewartet und neu entdeckte Sicherheitslücken werden nur in neueren Versionen behoben. Das Betreiben veralteter Dienste macht eine Organisation anfällig für Cyber-Angriffe und Dienstausfälle. Dieser Dienst sollte auf die neueste Version aktualisiert werden. Weitere Details finden Sie auf der PPTP Website. Dieser Dienst verwendet den Port 1723 auf der IP-Adresse xxx.

#4 Öffentlich sichtbare Dienste

Öffentliche/unbesicherte Vermögenswerte
Kontrolle von Vermögenswerten
Ransomware
Sicherheit

example.com: Remote Desktop Protocol remote_desktop verwendet derzeit den Port 3389 auf der IP-Adresse example IP und ist direkt sichtbar und zugänglich vom Internet. Solche Dienste, die extern sichtbar sind, machen eine Organisation anfällig für Cyber-Angriffe, Datendiebstahl und Serviceausfälle. Dieser Dienst sollte so konfiguriert werden, dass er nur von internen Netzwerken oder über ein VPN zugänglich ist.

#5 Verwundbare Dienste

Öffentliche/unbesicherte Vermögenswerte
Kontrolle von Vermögenswerten
Ransomware
Sicherheit

Ihre Organisation hat 2 MySQL database Ports, die vom Internet aus sichtbar und zugänglich sind. Dies stellt ein erhebliches Risiko dar, da diese offenen Ports (Verbindungen) von Hackern ausgenutzt werden können, um Zugang zu erlangen, und so eine Organisation extrem anfällig für Cyber-Angriffe und Serviceausfälle machen können.

Diese offenen Ports sollten sofort hinter einer Firewall versteckt oder die Ports geschlossen werden.

Darüber hinaus sollten Sie Verfahren und Richtlinien einführen, um zu verhindern, dass diese Ports in Zukunft offen gelassen werden.

Die öffentlichen Ports sind:
- Port 3306 auf IP-Adresse example IP (zugänglich über pulse.example.com)
- Port 3306 auf IP-Adresse example IP (zugänglich über example.com)

#6 E-Mail-Spoofing-Richtlinie

Finanziell
Phishing
E-Mail
Ruf

3 Ihrer Domains haben keine DMARC-Richtlinie, um zu verhindern, dass gefälschte E-Mails in den Posteingang des Empfängers gelangen. Selbst wenn Sie Schutzlösungen für eingehende Mails haben, verhindern diese nicht, dass Kriminelle gefälschte E-Mails an Ihre Kunden, Lieferanten und andere wichtige Geschäftskontakte senden!

Wenn diese aktiv für Geschäftsemails genutzt werden, empfehlen wir die Implementierung einer mindestens "überwachenden" DMARC-Richtlinie, um über E-Mails informiert zu werden, die nicht von Ihren autorisierten Absendern gesendet werden:
`"v=DMARC1 p=none rua=mailto:[insertAddress]@example.com"`

Für Domains, die nicht für E-Mails verwendet werden, empfehlen wir die Implementierung eines DMARC-Datensatzes, der die Empfänger darüber informiert, E-Mails, die von diesen Domains gesendet werden, abzulehnen:
`"v=DMARC1 p=reject rua=mailto:[insertAddress]@example.com"`
Dies sollte zusammen mit einem SPF-Datensatz von `"v=sf1 -all"` implementiert werden, um anzugeben, dass diese Domains E-Mails senden.

Die Domains ohne DMARC-Richtlinie sind:
- @example.com
- @examplecompany.com
- @examplecompanyltdcom

#7 Sicherheitszertifikate

Exploits
Unterbrechung des Geschäftsbetriebs
Datendiebstahl
Abgelaufene Prozesse

Die ausstellenden Zertifizierungsstellen für die Zertifikate auf 3 Ihrer Subdomains wurden nicht vertraut.

Bei Verwendung eines Zertifikats von einer nicht vertrauenswürdigen Zertifizierungsstelle zeigen die wichtigsten Webbrowser den Besuchern eine Sicherheitswarnung an und verhindern, dass sie die Seite erreichen. Dies stellt ein Risiko für die Geschäftskontinuität und den Ruf dar.

Neue Zertifikate, die von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wurden, sollten sofort installiert werden.

Die Subdomains mit nicht vertrauenswürdigen Zertifikaten sind:
- remote.example.com
- example.com
- www.example.com

Artikel zur Berücksichtigung

KYND empfiehlt Ihnen, diese Punkte zu überprüfen, da sie ein Risiko für das Unternehmen darstellen können, wenn keine Schutzmaßnahmen oder Milderungen für sie vorhanden sind. Sie könnten jedoch bereits davon Kenntnis haben, sie könnten aus legitimen Gründen vorhanden sein, oder die Schwachstellen stellen möglicherweise kein aktives Risiko für Ihre spezifischen Konfigurationen dar. Durch das Durchsehen dieser Punkte zur Bestätigung ihrer Anwendbarkeit auf Ihre Einrichtung stellen Sie sicher, dass Ihre Organisation vor potenziellen Ausnutzungen sicher ist.

#8 Mögliche Probleme

- Verwundbare Vermögenswerte
- Unterbrechung des Geschäftsbetriebs
- Schadsoftware
- Ransomware

12 Ihrer Organisation's Microsoft Exchange smtpd email_infrastructure Dienste haben bekannte und hoch sichtbare Sicherheitslücken in einigen Versionen, aber wir konnten die von Ihnen verwendeten Version(en) nicht bestätigen.
Die Verwendung von Software mit einer bekannten Schwachstelle macht eine Organisation extrem anfällig für Angriffe und Dienstausfälle. Neu entdeckte Software-Schwachstellen werden öffentlich bekannt gegeben, um alle Benutzer der betroffenen Produkte zu warnen und als Teil des Lösungsprozesses für Softwareentwickler. Leider teilen Angreifer auch Tools und Techniken, die zur Ausnutzung dieser Schwächen verwendet werden können, sobald sie öffentlich bekannt gegeben werden. Dies kann innerhalb von Tagen oder sogar Stunden nach Bekanntgabe einer neuen Schwachstelle geschehen.

Wir empfehlen zu überprüfen, ob eine aktuelle Version dieser Dienste verwendet wird, da diese Versionen für KYND nicht sichtbar sind.

Wir empfehlen auch, ein Verfahren zur regelmäßigen Überprüfung der Aktualität der Software zu implementieren (zum Beispiel ein Register aller verwendeten Software, wo sie verwendet wird und wer für ihre Aktualisierung verantwortlich ist). Verzögern oder ignorieren Sie keine Aufforderungen zur Aktualisierung von Diensten, die von Softwareanbietern gestellt werden.

Die betroffenen Dienste können auf den folgenden Infrastrukturelementen gefunden werden:
- Port 25 auf IP-Adresse xxx (zugänglich über examplecom)
- Port 25 auf IP-Adresse xxx (zugänglich über example.com)
- Port 25 auf IP-Adresse xxx (zugänglich example.com)
- Port 25 auf IP-Adresse xxx
- Port 25 auf IP-Adresse xxx
- Port 25 auf IP-Adresse xxx
- Port 25 auf IP-Adresse xxx
- Port 25 auf IP-Adresse xxx
- Port 25 auf IP-Adresse xxx
- Port 25 auf IP-Adresse xxx
- Port 25 auf IP-Adresse xxx
- Port 25 auf IP-Adresse xxx

#9 Verwundbare Dienste

- Öffentliche/unbesicherte Vermögenswerte
- Kontrolle von Vermögenswerten
- Ransomware
- Sicherheit

KYND hat festgestellt, dass 2 der FTP server file_server Dienste Ihrer Organisation direkt aus dem Internet zugänglich sind. Obwohl dies aus legitimen Gründen vorhanden sein könnte, könnte das Vorhandensein bestimmter Ports (Verbindungen), die direkt sichtbar und zugänglich aus dem Internet sind, ein Risiko darstellen und von Hackern ausgenutzt werden, um Zugang zu erlangen.

Wenn diese Ports öffentlich zugänglich sein sollen, möchten Sie vielleicht trotzdem die Ports, auf denen Sie sie freigeben, auf nicht standardmäßige umstellen, um es Angreifern schwerer zu machen, sie zu finden. Alternativ könnten Sie den Port hinter einer Firewall verstecken.

Die öffentlichen Ports sind:
- Port 21 auf IP-Adresse xxx (zugänglich über example.com)
- Port 21 auf IP-Adresse xxx (zugänglich über example.com)

#10 Veraltete Software

- Verwundbare Vermögenswerte
- Unterbrechung des Geschäftsbetriebs
- Schadsoftware
- Ransomware

2 Ihrer Organisation's MySQL database Dienste verwenden eine ältere Version dieses Produkts. Neuere Versionen von Produkten werden verfügbar, um sicherzustellen, dass alle Fehler oder Schwachstellen behoben sind, um maximale Sicherheit zu gewährleisten. Ältere Versionen von Diensten werden von ihren Entwicklern weniger gut unterstützt, was eine Organisation anfälliger für Cyber-Angriffe und Dienstausfälle macht.

Um optimale Sicherheit zu gewährleisten und Cyber-Angriffe zu verhindern, könnte eine neuere Version dieser Dienste vorzuziehen sein. Weitere Details finden Sie auf der MySQL Website.

Die betroffenen Dienste finden Sie auf den unten aufgeführten Infrastrukturelementen:
- Port 3306 auf IP-Adresse xxx (zugänglich example.com)
- Port 3306 auf IP-Adresse xxx (zugänglich example.com)

KYND START

#11 Verwundbare Dienste

Öffentliche/unbesicherte Vermögenswerte
Kontrolle von Vermögenswerten
Ransomware
Sicherheit

KYND hat festgestellt, dass 3 der OpenSSH developer_access Dienste Ihrer Organisation direkt aus dem Internet zugänglich sind. Obwohl dies aus legitimen Gründen vorhanden sein könnte, könnte das Vorhandensein bestimmter Ports (Verbindungen), die direkt sichtbar und zugänglich aus dem Internet sind, ein Risiko darstellen und von Hackern ausgenutzt werden, um Zugang zu erlangen.

Wenn diese Ports öffentlich zugänglich sein sollen, möchten Sie vielleicht trotzdem die Ports, auf denen Sie sie freigeben, auf nicht standardmäßige umstellen, um es Angreifern schwerer zu machen, sie zu finden. Alternativ könnten Sie den Port hinter einer Firewall verstecken.

Die öffentlichen Ports sind:
- Port 22 auf IP-Adresse xxx (zugänglich über pulse.example.com)
- Port 22 auf IP-Adresse xxx (zugänglich über example.com)
- Port 22 auf IP-Adresse xxx (zugänglich über example.com)

#12 Domain-Registrierung

Kontrolle von Vermögenswerten
Unterbrechung des Geschäftsbetriebs
Ruf
Abgelaufene Prozesse

5 Ihrer Domains haben unvollständige Daten über ihren Registranten: In diesem Fall war keine Registranten-E-Mail-Adresse von Ihren Registraren verfügbar.

Wir empfehlen Ihnen, Ihre Registrare zu kontaktieren und zu bestätigen, dass die E-Mail-Adressen der Registranten korrekt erfasst sind. Registranten-E-Mail-Adressen sollten keine persönlichen oder individuellen Firmen-E-Mail-Adressen sein, da diese ein erhebliches Risiko für die Kontrolle und Sicherheit der Domains darstellen. Wir empfehlen, dass die E-Mail-Details des Registranten für Ihre Domains eine Firmen-E-Mail-Alias sein sollten. Zum Beispiel könnten Sie domainadmin@[meinefirmenwebsite.com] verwenden.

Die Domains mit unvollständigen Daten über ihren Registranten sind:
- aexample..com
- example.net
- example.com
- e.xample.com
- examplecompany.net

#13 Domain-Ablauf

Kontrolle von Vermögenswerten
Unterbrechung des Geschäftsbetriebs
Ruf
Abgelaufene Prozesse

Die Domain-Registrierung für arbilling.com läuft am 2025-10-02T19:53:49Z ab. Wenn sie abläuft, funktionieren möglicherweise Dienste, die auf dieser Domain gehostet werden, nicht mehr und die Domain könnte von Cyber-Kriminellen übernommen und geklont werden, um Mitarbeiter und Kunden zu betrügen. Die Registrierung für diese Domain sollte so schnell wie möglich erneuert werden.

#14 Sicherheitszertifikate

Exploits
Unterbrechung des Geschäftsbetriebs
Datendiebstahl
Abgelaufene Prozesse

Die Zertifikate auf 5 Ihrer Subdomains enthalten die Subdomain nicht in ihren gültigen Namen. Zertifikate sind nur für die Subdomains gültig, die sie in ihrer Liste der gültigen Namen enthalten. Besucherverbindungen zu diesen Subdomains sind unsicher, selbst wenn sie später auf eine sichere Seite umgeleitet werden. Dies ermöglicht es Angreifern, das zu sehen und zu ändern, was sie auf der Seite sehen oder an die Seite senden. Und wenn ein Besucher zu einer dieser Subdomains navigiert, kann sein Browser eine Sicherheitswarnung anzeigen und ihn daran hindern, die Seite zu erreichen. Dies stellt ein Risiko sowohl für die Sicherheit als auch für das Kundenvertrauen in Ihre Website dar.

Ein Zertifikat, das für Ihre Subdomains gültig ist, sollte ausgestellt und auf 5 Ihrer Subdomains installiert werden.

Die von diesem Problem betroffenen Subdomains sind:
- aexample..com
- example.net
- example.com
- e.xample.com
- examplecompany.net

Domänen

Dies sind die Domains, die KYND als von Unternehmen registriert identifiziert hat.

Domain	Registrierungsdetails	Risiken	Unterdomänen
example.net	**Registrierungs-E-Mail:** jdoe@example.com **Organisation des Registranten:** Example, LLC **Registrar:** EXAMPLE DOMAINS INC	00 Hohe Risiken 01 Betrachten 04 Gut!	02
example.com	**Registrierungs-E-Mail:** https://www.godaddy.com/whois/results.aspx?domain=example.com&action=contactDomainOwner **Organisation des Registranten:** Example, LLC **Registrar:** example.com, LLC	00 Hohe Risiken 01 Betrachten 04 Gut!	05
example.com	**Registrierungs-E-Mail:** jdoe@example.com **Organisation des Registranten:** Example Company **Registrar:** EXAMPLE DOMAINS INC.	00 Hohe Risiken 01 Betrachten 04 Gut!	03
example.net	**Registrierungs-E-Mail:** jdoe@example.com **Organisation des Registranten:** Example LTD **Registrar:** EXAMPLE DOMAINS INC.	00 Hohe Risiken 01 Betrachten 04 Gut!	02
example.com	**Registrierungs-E-Mail:** jdoe@example.com **Organisation des Registranten:** EXM CO. **Registrar:** EXAMPLE DOMAINS INC.	00 Hohe Risiken 02 Betrachten 03 Gut!	03