Think Your Databases Are Safe? Think again

Tony Davis & Grant Fritchey
Redgate Software
Goals

Understand the threats our databases are under

Learn how SQL Monitor can better protect your estate
Grant Fritchey

🔗 scarydba.com

📧 grant@scarydba.com

🐦 @gfritchey

📺 youtube.com/c/GrantFritchey
Compliant Database DevOps

Deliver value quicker while keeping your data safe

- Standardize
  - team-based development
- Automate
  - database deployments
- Protect
  - & preserve data
- Monitor
  - performance & availability
SQL Monitor & Estate Monitoring
SQL Injection Vulnerability

• Top 10 vulnerability according to OWASP & CVE
• #14 vulnerability according to Whitehat Security
<table>
<thead>
<tr>
<th>Date Made Public:</th>
<th>November 30, 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company:</td>
<td>Marriott International</td>
</tr>
<tr>
<td>Location:</td>
<td>Maryland</td>
</tr>
<tr>
<td>Type of breach:</td>
<td>HACK</td>
</tr>
<tr>
<td>Type of organization:</td>
<td>BSR</td>
</tr>
<tr>
<td>Records Breached:</td>
<td>327,000,000</td>
</tr>
</tbody>
</table>

Marriott International disclosed a massive security breach of the reservations system for its Starwood Hotels and Resorts brand, a hack it said Friday may have compromised private info on up to 500 million guests.

According to Marriott, for around 327 million Starwood guests, the database included such personal information as name, mailing address, phone number, email address, passport number, date of birth, and gender. For some Starwood customers, the hacked database also stored payment card numbers and expiration dates, although Marriott said that information was encrypted.

*Information Source: Media*

https://answers.kroll.com/
Indio Water Authority notifies residents of Click2Gov breach

In reviewing the Click2Gov breaches, I just discovered another one from October that I hadn’t posted on this site. Let’s remedy that now. Statement on Click2Gov Data Security Incident INDIO, CA (October 12, 2018) – Indio Water Authority (IWA) was informed in September of a cybersecurity incident potentially affecting the credit card information of customers [...]

Data Breaches: Databreaches.net
Compliant Database DevOps
Deliver value quicker while keeping your data safe

Standardize
team-based development

Automate
database deployments

Protect
& preserve data

Monitor
performance & availability
SQL Injection & SQL Monitor
What you should be doing

- Least Privilege
- Principal
- Scatter Sensitive Data
- Sanitize Input
- Monitor for SQL Injection
Monitoring For SQL Injection

- Monitor for errors linked to SQL injection
- Track changes to permissions
- Monitor SQL server configuration settings
- Watch for database drift
Product Learning At Redgate

Product articles
Tips and how-to guides for Redgate products

Goals

Understand the threats our databases are under

Learn how SQL Monitor can better protect your estate