hospitalitynet™

Will Marriott data breach herald the death of personalization?

By Greg Abbott, VP Travel & Hospitality at DataArt

4 min0 Comments

This analysis could be titled in a number of ways, each with a lean towards what was disclosed by Marriott last week when it emerged some 500 million guest accounts had been hacked.

Because of the size of the breach and the underlying issues that may have caused it, many may point to the hotel sector's drive towards personalization and trigger a major rethink.

Alternatively, stopping the next Marriott-like data breach may simply be a question of implementing many of protocols and strategies outlined below.

Or, perhaps, it's more of a rallying cry for stronger legislation - at least in the U.S. - which will ensure that brands across the travel spectrum take security (more) seriously.

But first some background...

I recently attended The Phocuswright Conference, where some of travel tech's mightiest flock to debate industry trends. Apart from a few companies that are leveraging machine learning to battle the "black hat" hackers, security was absent from the agenda.

It was not on a single marquis, nor was it the subject of a hot debate or an executive interview. Let's face it, as far as tagline topics go… "security" may be one of the least exciting topics at a conference covering the market's leading innovation.

In short: despite the growing number and scale of security breaches, hospitality companies are still slow to invest in security.

But why?!

A number of factors may be at play.

First of all, there is no upside to security. It doesn't drive new revenue or customer acquisition, making the "cost" of increased security measures difficult to justify (until now, anyway).

Furthermore, hotels' complex, distributed IT systems (internet booking engines, distribution systems, customer relationship management and hotel local systems) call for sophisticated, multi-dimensional, and expensive security measures.

Below are some ways that hospitality companies can improve their security and avoid data breaches.

Personally identifiable information (PII) has become the new target for attackers, and organizations are still making too little effort to protect it.

PII is often duplicated across multiple systems, un-encrypted, and kept longer than needed and can be easily exported in bulk.

A sensible approach for handling PII is data "pseudonymization" whereby personal information is transferred to a separate database with adequate security controls (encryption, access control, audit, etc.) and each person is assigned a unique ID.

All other systems operate with unique IDs instead of actual PII, which can be retrieved via a separate process. Any PII that is not required for immediate business needs should be deleted or archived.

Most organizations focus on their perimeter security at the expense of breach detection and response within the internal network.

They simply ignore the fact that attackers need only find a single flaw in a vast landscape, while defenders need to cover the entire attack surface. Even if they do so, there is a range of "unfair" attack methods, including social engineering, zero-day flaws, and insider attacks, that are not possible to cover by perimeter defense.

Hotels need subscribe to regular audits and penetration testing of their infrastructure, both internal and external.

Red pill, not the blue pill

A recent trend among advanced organizations is to employ "red teams," which are independent groups that take the adversarial point of view and challenge the effectiveness of a security program.

"Red teams" use various techniques, including social engineering, phishing, or posing as a company employee, to penetrate the internal network. During such simulated attacks, companies get a realistic view of their defense capabilities.

Traditional perimeter defenses such as firewalls, IDS/IPS, patching, anti-virus, etc, are still required, but IT security teams need to go further, assuming that the perimeter is compromised and taking a proactive approach to detecting malicious activity.

Here are some essential controls that are often overlooked but can massively improve security:

- Enable outbound traffic filtering where possible, as it allows detection of attackers when they attempt to copy the stolen information to their servers.
- Deploy group policies on non-IT staff computers that detect suspicious activity such as running PowerShell, opening a reverse-shell, making network attacks, etc.
- Run regular social engineering simulation exercises to train the staff to react appropriately.

- Update password policies that check new passwords against dictionary words or common patterns that attackers use during brute-force attacks (in most attacks, after the perimeter is bypassed, attackers access accounts with weak passwords).
- Enforce MFA for privileged accounts and sensitive areas.
- Collect audit logs from various sources and ship them to a central secure server with separate access control.

Finally, I submit that it is time for the U.S. - home to some of the largest and most advanced technology companies in the world - to introduce legislative data security measures and force the travel industry to take data protection seriously.

The evolving nature of cyber threats calls for a continuous legislative effort as well as for collaboration with other governments, industries, and academia.

At the time when personalization is a critical driver of innovation and progress, it is imperative that data security takes center stage.

This article was first published on phocuswire.com

About DataArt:

DataArt is a global technology consultancy that designs, develops and supports unique software solutions, helping clients take their businesses forward. Recognized for their deep domain expertise and superior technical talent, DataArt teams create new products and modernize complex legacy systems that affect technology transformation in select industries.

DataArt has earned the trust of some of the world's leading brands and most discerning clients, including Nasdaq, S&P, United Technologies, oneworld Alliance, Ocado, artnet, Betfair, and skyscanner. Organized as a global network of technology services firms. DataArt brings together expertise of over 2,200 professionals in 20 locations in the US, Europe, and Latin America.

www.dataart.com

@dataart

Source: https://www.hospitalitynet.org/opinion/4091350.html