German
Business Protection

Risk Consultancy
Business Enablement
Compliance & Security

Security Threats Germany

March 2017

Berlin, March 13th 2017

Hotline	+49 30 63967027-0
Fax	+49 30 63967027-99
E-Mail	info@gbp-security.com
Internet	gbp-security.com

How Security Lapses can Impact the Value of your Brand

It is often talked about the "value" of a brand - but what does it actually consist of? The value of a brand does not only consist of the financial ratios and valuations. Brand Value can best be described as the sum of how much people will choose one brand over the alternatives. People are willing to pay over the odds for a desirable product, such as Apple's Iphone, even if the alternatives have an identical performance. Strong brands can command a premium, resulting in high profits for the owner.

It takes time to build up a strong brand; however the value of a brand can disappear very rapidly if the positive perception of the product or service is put into doubt. In the past brands lost value due to such events as product recall, product failure or lack of reliability, as one could see impressively with Volkswagen, whose market value had fallen by more than 50% after the acquaintance of the exhaust gas scandal, and the worldwide slide of reputation of the VW brand.

The age of Internet has added a further dimension to the issue of protecting brand value. Today websites and web applications are the most visible and increasingly vulnerable part of a company`s infrastructure. It is no surprise that cybercriminals scan thousands of websites in search of vulnerabilities.

When a security breach occurs, it`s not just consumer data that is compromised. If it becomes known that a breach has occurred, consumer confidence and trust in the brand also falls resulting in falling sales and loss of revenue. This can translate into long-term declines in revenues and subsequently massive investments to regain consumer confidence. Such breaches make big headlines when big brands are involved. As an example, the security vulnerabilities discovered on Samsung Smart-TV a few days ago, which will possibly again have a negative effect on the sales figures as well as on the image of the brand Samsung.

This leads many SME`s to think that just because they are small this makes them immune to such threats. Such companies should assume that they too are equally under threat from cyber criminals. Given that such companies do not have the financial resources large companies can muster, the threat to SME`s financial existence is in fact larger.

This makes it crucial for SME`s to take the problem seriously and act proactively to deter cyber criminals. This means that the work force needs to be made aware of the importance of following clear rules when handling sensitive client data. Adopting BSI basic protection concept or the ISO 27001 as a bench mark are sensible first steps; they do, however, need to be lived by all in the company. Establishing a clear protocol is crucial as is a constant monitoring of new scams and methods employed to breach your company’s cyber defenses. Technology helps, but don`t forget that it is the employee who is the weakest link in the defense of your data. Make sure that only suitably vetted and screened personnel can access sensitive data and above all, adjust the level of data security to the threat level.