Threats By Numbers

The majority of retailers were victims of a cyber-attack in 2015

55% of all retail firms were hit by cybercriminals in 2015. The growing prevalence of e-commerce and the preponderance of credit card information stored by retailers has made them a tantalizing target for hackers.

Data breaches in the retail industry cost more

The average cost per record stolen for retailers is $172. This is significantly above average, and more expensive than data breaches in energy, technology, or media.

Cyber Defense for Retail & E-Commerce

With many high-profile cyber-attacks against major household names including Target, Home Depot, and Neiman Marcus, retailers have become increasingly concerned with cyber security in recent years.

While the immediate effects of such attacks can be measured by the financial losses suffered by these organizations in repairing the damage, there is also a longer term impact, as high-profile breaches significantly undermine customers’ trust in retailers who have been hacked.

Customer data has been a primary target of many attacks, as it can quickly be monetized. Because retailers store and process such large volumes of consumer data, they are particularly at risk. In an effort to protect consumers, the EU’s General Data Protection Regulation requires retailers to pay heavy penalties if theft of customer data is not reported within 72 hours.

Given their reliance on e-commerce, retailers are also particularly vulnerable to distributed denial-of-service attacks or website hacks. In late 2016, a DDoS attack on DNS server Dyn took many popular websites offline, including retailers such as Amazon and Etsy. Similarly, attackers are taking advantage of retailers’ dependence on supply chains in order to breach their networks.

Finally, insider threat poses a perpetual risk to retail firms. At the supermarket chain Morrisons, for instance, a disgruntled employee released financial records of 100,000 staff members, leading to an estimated $2.6 million lawsuit. Moreover, insider threats are not always malicious. Users can be tricked into giving away their login credentials, or they could click on a suspicious link in a phishing email.

Defending our customers’ sensitive data against cyberattack is of the utmost importance and Darktrace has enabled us to do it.

Stephen Antell, CISO, Rentalcars.com
Darktrace’s Enterprise Immune System has given us peace of mind that we are well-equipped to defend against today’s sophisticated attacks.

Dane Sandersen, Global Security Director, Trek