Data Breach of the Security Platform Suprema BioStar 2

Table of Contents

Page

List of Figures

Page

1 Introduction

A data breach is a "compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed". (British Standards Institute, 2016)

BioStar 2 is a web-based security platform, developed by Suprema, that allows for access control, attendance and visitor management. The service provides a biometric security smart lock platform which allows admins to control access to secure areas of facilities, to see activity logs and their history, for example, logging who and when someone enters and exits a building, and managing users and their permissions - the users being the employees of companies. The BioStar 2 uses biometrics such as facial recognition and fingerprinting technology to identify users. (vpnMentor, 2019; Suprema, 2021)

Suprema was named one of the world's top 50 security companies and the sole dedicated biometrics provider in 2018. They have partnered with Nedap to integrate BioStar 2 into their AEOS system. Nedap provides the AEOS service to over 5700 organizations in 83 countries to banks and businesses ranging in size from small and local to some of the biggest multinational businesses. Moreover, it is also used by government agencies such as the Metropolitan Police, the European Parliament and The Scotland Yard. (ACNNewsWire, 2018; vpnMentor, 2019; Nedap Security, 2021)

The data breach in the security platform BioStar 2's database has exposed 27.8 million of unsecured records. The breach comes to a total of 23 gigabytes of data, all of which is highly sensitive. All of which could come from any of the organizations listed previously, which is deeply concerning. The records hold unencrypted user credentials and unencrypted personal information of employees, for example their address, fingerprint records and facial recognition information. (vpnMentor, 2019)

2 Timeline of the Breach

The breach was discovered by vpnMentor's team, which is led by the internet privacy researchers Noam Rotem and Ran Locar. The breach was only discovered on the 5th of August 2019. The BioStar 2 platform was launched by Suprema on the 11th of March 2015, suggesting that the risk of a data breach could have been lingering in the flawed security platform for the better part of four years. vpnMentor did analyze bits and random files from the breach, however they did not download every file they discovered in the breach because of ethical reasons. They limited the invasion of privacy of all the innocent employees all while proving that, from what files they've downloaded, the whole dataset has been compromised. Either way, a large amount of biometric data was now available online, breaching GDPR. (Suprema, 2015; BBC News, 2019; Verdict, 2019)

Suprema was contacted by vpnMentor about the data breach on the 7th of August 2019. vpnMentor tried to raise attention to the very dangerous data breach however they were dismissed by Suprema. Specifically, their German branch of the company told the team that they "don't speak to vpnMentor" (vpnMentor, 2019). Almost all the other attempts to try to contact Suprema about the data breach were met with unresponsiveness and uncooperativeness. Luckily, the French branch of Suprema was more cooperative, and after the team at vpnMentor spoke to them, they took steps to close the breach. The breach was effectively closed on the 13th of August 2019. (vpnMentor, 2019)

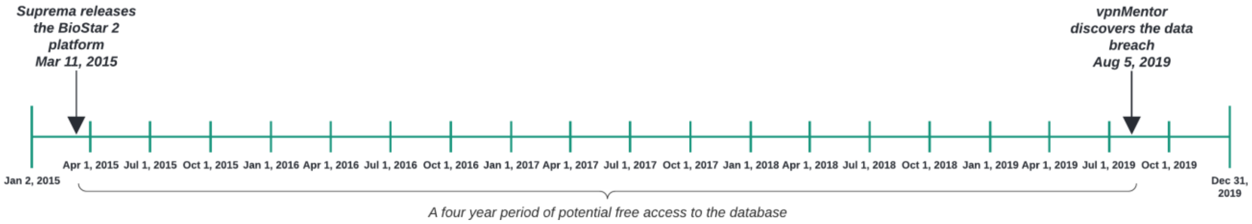

Figure 2-1 - A four-year timeline of the BioStar 2

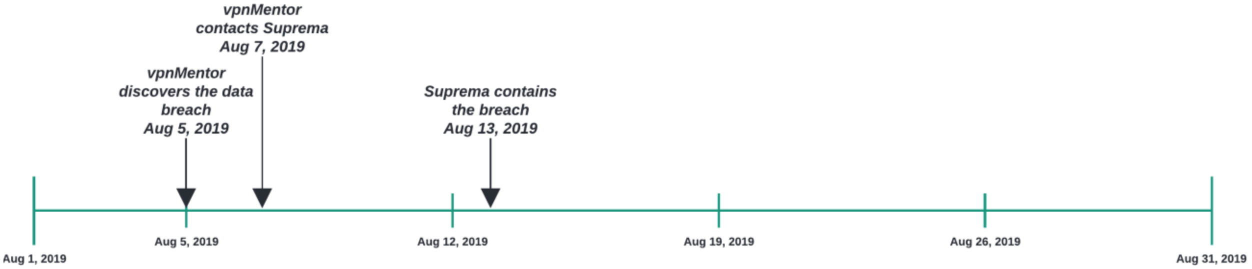
vpnMentor contacts Suprema Aug 7, 2019
vpnMentor discovers the data breach Aug 5, 2019
Suprema contains the breach Aug 13, 2019
Aug 1, 2019
Aug 5, 2019
Aug 12, 2019
Aug 19, 2019
Aug 26, 2019
Aug 31, 2019

Figure 2-2 - Timeline of the breach

3 Identifying Relevant Information Risks

The data breach of the BioStar 2 security platform has been caused by many overlooked simple information security principles. The BioStar 2's custodians and owners of the information assets seem to have completely breached the first principle of the CIA triad, Confidentiality. They have successfully put all their information assets at risk. Confidentiality is "the property that information is not made available or disclosed to unauthorized individuals, entities or processes" (Sutton, 2014, p. 18). As a result, there should have been measures that prevent sensitive information from unauthorized access attempts. The information assets were simply hidden by their hierarchical system as the BioStar 2 platform is, of course, separating users from administrators. Regardless, the information was easily available to unauthorized individuals who knew where to look. Even more so, crucial information assets were simply stored in plain text. (WhatIs.com, 2021; vpnMentor, 2019)

For example, vpnMentor was able to access the following:

1. **Free access to client administrator panels,**

A threat actor with access to an administrator panel could add and remove users or edit users' details, essentially taking over accounts, likely to give themselves access to buildings.

2. **Free access to client dashboards,**

Free access to the dashboards could be useful to the threat actors to understand an organization's infrastructure, allowing them to perform reconnaissance.

3. **Access to client back-end controls,**

A threat actor could change an organization's back-end controls, such as the security rules, to make it easier for themselves to access a building, compromising the organization's security.

4. **Access to client permissions,**

A threat actor could give themselves the highest permissions available to gain a great amount of control over the organization.

5. **Unencrypted fingerprint data, facial recognition information and images of users,**

A threat actor could directly take the biometric data of people, making a library of fingerprints and facial recognition information that could be used for various crimes such as impersonation and fraud.

6. **Unencrypted usernames, passwords and IDs,**

A threat actor could take over users' organization accounts and other accounts as some might use the same password. Account data should be encrypted with a non-reversible algorithm such as a hash. (Strahs, 2009)

7. **Access to records of entry and exit to secure areas,**

A team of threat actors can help to infiltrate a building covertly. A threat actor enters then exits a building with forged documents, then another deletes the log of the entry and exit.

8. **Access to employee records, employee security levels and clearances,**

Threat actors could use the records to forge documents or to take over their accounts.

9. **Free access to unencrypted personal details, including employee home address and emails,**

A threat actor could use this information to compile a library of personal details that could be used for forgery and identity theft. Moreover, they could gain access to users' email accounts by using the unencrypted passwords - if their accounts use the same passwords.

10. Access to business' employee structures and hierarchies,

Threat actors could gain information of the organization's structure to give themselves the highest access available, since they also have access to the administrator panels.

11. Mobile device and OS information,

A threat actor could use this information to know exactly what type of scripts to use to exploit vulnerabilities of the specific operating system and/or mobile device to gain access to the device.

4 Analysing an Identified Risk

The threat actor gaining access to the administrator panels could be deemed incredibly catastrophic for an organization. Leaving an administrator panel unprotected could mean that a threat actor would easily be able to access all the employees of an organization and their details – including their account details and their personal details such as their addresses.

4.1 Asset Affected

The asset affected in this case would be the employees' details. The details include their account details – their user IDs, usernames and passwords – and their personal details – addresses, biometrics (fingerprints and facial recognition data) and images of them.

4.2 Vulnerability

The breached database contained the information of all their clients' administrator panels credentials unencrypted. The credentials were simply encoded in Base64, which was easily reversible. (Verdict, 2019)

4.3 Threat

A threat actor could compile a library of credentials for the administrator panels of multiple high-profile organizations and governmental organizations, compromising their security. They would then have access to the employees' credentials of each organization collected.

4.4 Threat Actor

vpnMentor did not have any malicious intent when discovering this data breach. According to them, they look for vulnerabilities that would lead them to a data breach as part of a "huge web-mapping project". (vpnMentor, 2019) However, there might exist other threat actor or perhaps multiple threat actors as the database was unsecured for a long time. It is unclear if any malicious actors accessed the data while it was unsecured. (The Verge, 2019)

4.5 Impact

The threat actor(s) could use the details collected to compromise the security of the organizations. For example, they could use the credentials to gain access to high-clearance officials and expose top secret governmental documents, which could put the country's safety at risk. Moreover, they could compile the employees' personal details for various crimes such as identity theft and fraud.

4.6 Likelihood

The likelihood of the risk is uncertain because there isn't a threat actor that has been publicly identified to have taken advantage of the breach. Moreover, it is unclear whether any threat actors have accessed the data while it was unsecured. However, Suprema's BioStar 2 was released in 2015 and the breach was discovered in 2019. In the span of four years, perhaps a threat actor may have been collecting the data from the breach and they may have been collecting documents from the compromised organizations. On-the-other-hand, the data breach may have gone completely under the radar.

5 Potential Consequences

Suprema had to deal with plenty of consequences, social and economic. Economically, the organization could lose a lot of high-profile stakeholders, such as the Metropolitan Police. However, based on Suprema's partner's website, Nedap, they are still listed as one of their partners, along with other government organizations such as the European Parliament and Nedap are still partnered with Suprema, even after the data breach that tainted their reputation. Losing such high-profile stakeholders could have a knock-on effect on other stakeholders in the company. The high-profile stakeholders would get publicized in newspapers, bringing more attention to the breach, which could cause smaller stakeholders to question the success of Suprema, ultimately leaving it for another security company. (Nedap Security, 2021)

Suprema breached the CIA triad by having this database unprotected. Specifically, they breached the confidentiality principle directly by having an unprotected database of credentials, easily accessible by any threat actor. Potentially, the integrity principle could be breached as a threat actor would be able to change the personal or account details of any employee of any of Suprema's stakeholders. Precisely, a threat actor could add, delete and modify any new us they'd like, which would breach the integrity principle by definition. (Sutton, 2014)

The availability principle could also be potentially breached. Hypothetically, as the security platform would need maintenance or updates, an administrator panel would have access to shut down the security platform for such tasks. Therefore, a threat actor with access to an administrator panel would be able to shut down the access to the data, effectively breaching the availability principle.

"*Facial recognition and fingerprint information cannot be changed. Once they are stolen, it can't be undone*." (vpnMentor, 2019) This is why the BioStar 2 breach is so dangerous. Instead of saving hashes of facial recognition and fingerprint information, they are saving people's actual biometric information. All this unsecured data can be used by criminals for all sorts of illegal activities. The personal biometric details can be sold on the dark web for other criminals to use for illegal financial gain. The danger is that once one's fingerprint is stolen, a fingerprint cannot be changed.

Suprema's actions cause consequences at the stakeholder's end, impacting each and every one of their partners' security. With the data leak, a threat actor and their team have full access to administrator accounts on the BioStar 2 platform. The team of hackers can take over one of the organization's admin accounts that has high-level permissions and security clearances. As a result, the hackers can change the security settings of a whole network. Moreover, they can change user permissions, locking people out of specific areas in a building and they can create new accounts, adding their own facial recognition and fingerprints to give themselves access to an organization's building. The team of threat actors can also change the biometric data of existing accounts, essentially hijacking a user's account to access buildings undetected. Combining this with the fact that they have access to activity logs, where they can delete or change the information collected to hide their activities, the hacked building's security infrastructure is futile. The hackers would have free, undetectable movement within the organization, physically, in buildings or facilities, and on the internet. (vpnMentor, 2019)

With this newfound access, the hackers can just walk into a room into any building and just steal any sort of valuable object, information, install keyloggers, install viruses, it is up to their imagination since they essentially have gained full control. They can now do this to any closed network in the building as well, as they now have access to it. The employees' personal details such as their images, names, employment records, email addresses and home addresses are also accessible by the hackers, which the threat actors can use for identity theft. The details can also be used for phishing attacks inside the organization. The attackers can imitate an honest email and embed malware to steal information. The email would be effective as it would come from a genuine employee inside of the organization, making the attack exponentially more likely to succeed. Certain individuals with access to an asset of interest to the threat actors could get blackmailed or extorted. This helps the actors gain important information without putting themselves in danger by collecting it themselves, either online or physically. BioStar 2's database shows individual security clearances so the hackers can target employees with high-level access. They have access to personal information, which could make this type of attack very effective. This places innocent employees under an inexcusable amount of danger. (vpnMentor, 2019)

Regarding GDPR, there is no evidence that the data was compromised by malicious threat actors, however the data breach will likely be found to fail to respect GDPR. According to the Information Commissioner's Office, according to Verdict, "had Suprema had failed to protect the data of EU citizens, the firm could face a maximum fine of up to 4% of global annual turnover". (Verdict, 2019)

6 References

ACNNewsWire (2018). *Suprema named to world's top 50 security companies, sole dedicated biometrics provider in 2018 A&S Security 50 Rankings* [Online] Available at: https://www.acnnewswire.com/press-release/english/48004/suprema-named-to-world's-top-50-security-companies,-sole-dedicated-biometrics-provider-in-2018-a&s-security-50-rankings (Accessed 23 November 2021)

BBC News (2019). *Biostar 2: Suprema plays down fingerprint leak reports* [Online] Available at: https://www.bbc.co.uk/news/technology-49418931 (Accessed 24 November 2021)

British Standards Institute (2016). BS EN ISO/IEC 27040:2016 *Information technology. Security techniques. Storage security,* p. 2. [Online]. Available at https://bsol.bsigroup.com/Bibliographic/BibliographicInfoData/000000000030333322 (Accessed 21 November 2021)

Nedap Security (2021). *Customer Stories* [Online] Available at: https://www.nedapsecurity.com/customer-stories/ (Accessed 23 November 2021)

Strahs, B. (2009). *Secure Passwords Through Enhanced Hashing Secure Passwords Through Enhanced Hashing.* [Online] Available at:

https://scholarworks.wm.edu/cgi/viewcontent.cgi?article=1251&context=honorstheses (Accessed 29 November 2021)

Suprema (2021). *BioStar 2* [Online] Available at: https://supremainc.com/images/upload/brochure/[SUPREMA-ASB-BS2-EN-REV09]_LowRES.pdf (Accessed 23 November 2021)

Suprema (2015). *Suprema Unveils BioStar 2, The New IP Access Control Platform* [Online] Available at: https://web.archive.org/web/20150323220039/https://www.supremainc.com/en/node/1670 (Accessed 23 November 2021)

Sutton, D. (2014). Information Risk Management: A practitioner's guide, BCS Learning & Development Limited, Swindon. Available from: ProQuest Ebook Central. (Accessed 25 November 2021)

The Guardian (2019). *Major breach found in biometrics system used by banks, UK police and defence firms* [Online]. Available at: https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms (Accessed 21 November 2021)

The Verge (2019). *Huge security flaw exposes biometric data of more than a million users* [Online] Available at: https://www.theverge.com/2019/8/14/20805194/suprema-biostar-2-security-system-hack-breach-biometric-info-personal-data (Accessed 26 November 2021)

vpnMentor (2019). *Report: Data Breach in Biometric Security Platform Affecting Millions of Users* [Online]. Available at: https://www.vpnmentor.com/blog/report-biostar2-leak/ (Accessed 21 November 2021)

Verdict (2019). *Suprema data breach: What GDPR says about biometrics* [Online] Available at: https://www.verdict.co.uk/suprema-data-breach-gdpr/ (Accessed 24 November 2021)

WhatIs.com (2021). *confidentiality, integrity and availability (CIA triad)* [Online] Available at: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA (Accessed 26 November 2021)