QuickBit

Data Exposure Incident Report

2019-07-26

Technical specifics and other confidential information have been redacted from this public version of the incident report.

This report is bilingual, with the first section in English and the second section with the same content in Swedish

---

Denna rapport är tvåspråkig, med den första delen på engelska och den andra delen med samma innehåll på svenska

QuickBit eu AB (publ) – Kungsgatan 8, 2tr – 111 43 Stockholm – Sweden
www.QuickBit.eu

QuickBit

Table of Contents

(

(

QuickBit

1. Author and Contact Information	
Company Name	QuickBit eu AB (publ)
Document Title	Data Exposure Incident Report
Date	Friday, July 26, 2019
Author	Chief Technology Officer
Contact for any queries regarding this report	Managing Director Jörgen Eriksson E-mail: jorgen.eriksson@quickbit.eu Telephone: 0046-70-681 2777

(

2. Summary

2.1 QuickBit eu AB (publ)

QuickBit eu AB (publ) ("QuickBit") is a Swedish financial technology company with business operations located at Gibraltar. The Company provides e-commerce merchants internationally with technology solutions for blockchain and crypto-currencies. QuickBit is a public company listed on the NGM Nordic MTF market.

As a part of the Company´s customer solutions, QuickBit maintains a crypto-currency inventory in Bitcoin, Bitcoincash and Litecoin, selling from its own inventory.

2.2 Data exposure incident

On Monday July 15th 2019, QuickBit was made aware of a vulnerability on one of the Company´s servers. The server made an internal database and its contents visible for search from the Internet.

The server contained a third-party system which had been delivered in source code format by a software solution vendor. Whilst QuickBit technicians initiated server provisioning, deployment of code, starting of the database/services and loading of data, this was done on a virtual server outside of the production environments firewall.

Then the database was erroneously populated for testing purposes with a limited subset of production environment data. The exposed database contained customer records which QuickBit stores as a part of ongoing business.

301 398 data events were exposed, related to 17 060 customers from 50 countries. This does not mean that this number of transactions were exposed. A number of "data events" together combines into one transaction, or attempted transaction, which may be approved or rejected by the systems for security issues, attempted fraud or incomplete information.

Overall, data was exposed for approximately 2% of QuickBits total number of customers. Of these 17 060 exposed, a limited number (223 customers) were from European Union countries.

(

The exposed server was set up on QuickBits hosting platform in the Netherlands on June 16th 2019 and it was moved into the QuickBit firewall protected production environment on July 3rd 2019. This means that the data was exposed for 17 days.

The data exposure was discovered and documented by security researcher Bob Diachenko and editor Paul Bischoff at Comparitech Limited and QuickBit was made aware of the data exposure by an e-mail from James Agate, also at Comparitech.

As mentioned, the exposure ended after the new server was moved inside the company firewall on July 3rd. At the time when QuickBit was made aware of the exposure, immediate actions were taken to ensure that all servers and databases were safe, before an investigation was initiated. The investigation was conducted by QuickBit and the third-party system vendor and is documented in this public incident report.

There is no evidence that there has been any appropriation of data by anyone else than Comparitech, and no misuse or attempted use of the information exposed in this incident.

The exposed database records contained information about individual transactions and attempted transactions facilitated by the QuickBit platform, including name, address, e-mail, gender, date of birth, payment information (type of credit card used and first six and last four digits), source currency and target currency (for example, USD to BTC) and transaction amount.

Neither the company, nor its customers have suffered or can be foreseen to suffer any financial loss.

The exposed database did not contain any passwords or keys to any of the crypto-currency wallets.

Based on the results of our internal investigation, customers affected are in the process of being contacted with information about the incident. We are also reporting the incident to the Swedish Data Protection Authority and to the relevant parties in Gibraltar.

QuickBit regrets that this incident occurred and sincerely apologizes for any concern or distress the incident may have caused our customers. QuickBit is

(

committed to provide efficient, safe and secure services, whilst protection of personal customer information remains as a core focus.

We are reviewing our internal protocols and procedures to prevent this from happening again.

(

3. Classification of exposure

3.1 Breach or incident

The investigation documented within this report, concludes that QuickBit has been the victim of a cybersecurity incident

In the field of data security, the term *breach* is used to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to confidential information. It is our the conclusion that a *breach* did not occur.

Incident is a broader term describing an event that actually or *potentially* jeopardizes the confidentiality, integrity, or availability of a computer network or the information stored on or transmitted by the computer network.

Breach is a more narrow term that describes the actual loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access of information.

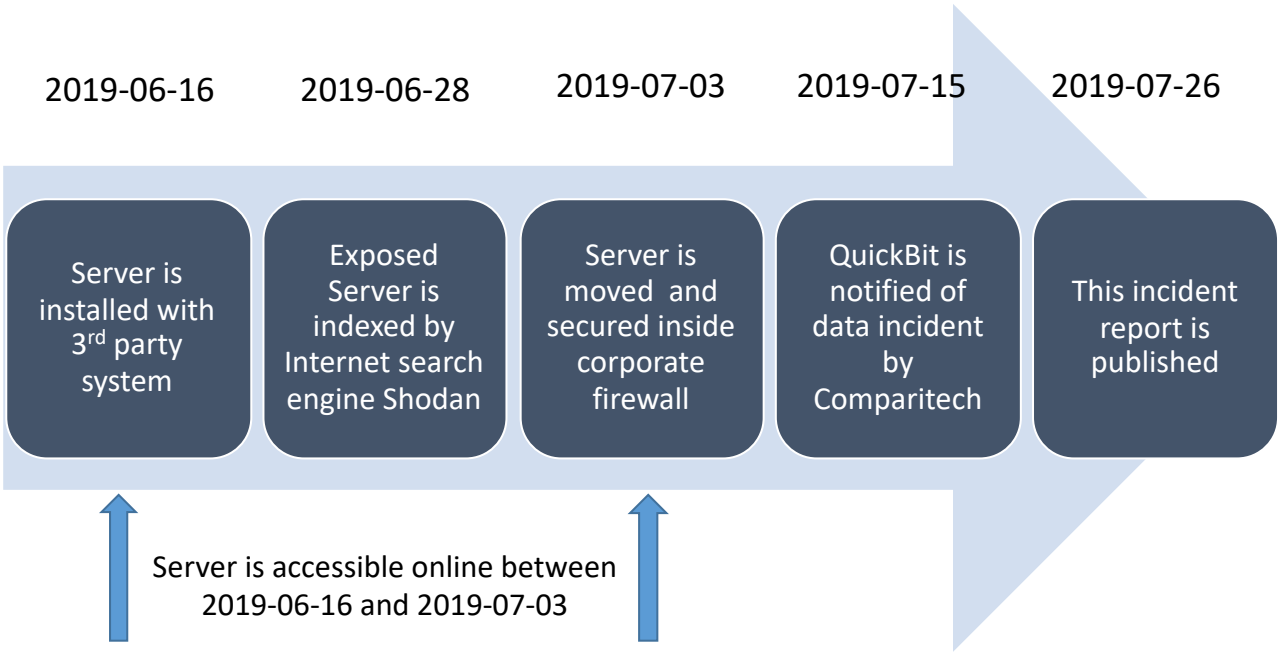
The data exposure documented within this report allowed for confidential data to be available outside of QuickBits firewall for a period of 17 days. According to our investigation, however, even though the data was exposed, it was only accessed by the security researchers that contacted QuickBit to let us know of the breach, and the data has not been spread further nor used for any malign purposes.

The security researchers first contacted QuickBit on July 2nd 2019. However, this notification was not noticed by QuickBit, as this initial e-mail was considered to be spam by our mail server and hence not read by anyone at QuickBit.

The e-mail that was sent to QuickBit´s Managing Director on July 15th was noticed and immediately acted upon.

(

4. Timeline



Comparitech wrote an e-mail to QuickBit on July 2nd, but this initial e-mail was not noticed as it was caught by the spam-filter in QuickBits e-mail system.

The new e-mail sent from Comparitech on 15th July to QuickBits Managing Director was noticed and immediately acted upon. By then the Server was already secured, as it was moved inside the firewall on July 3rd.

(

5. System and Architecture

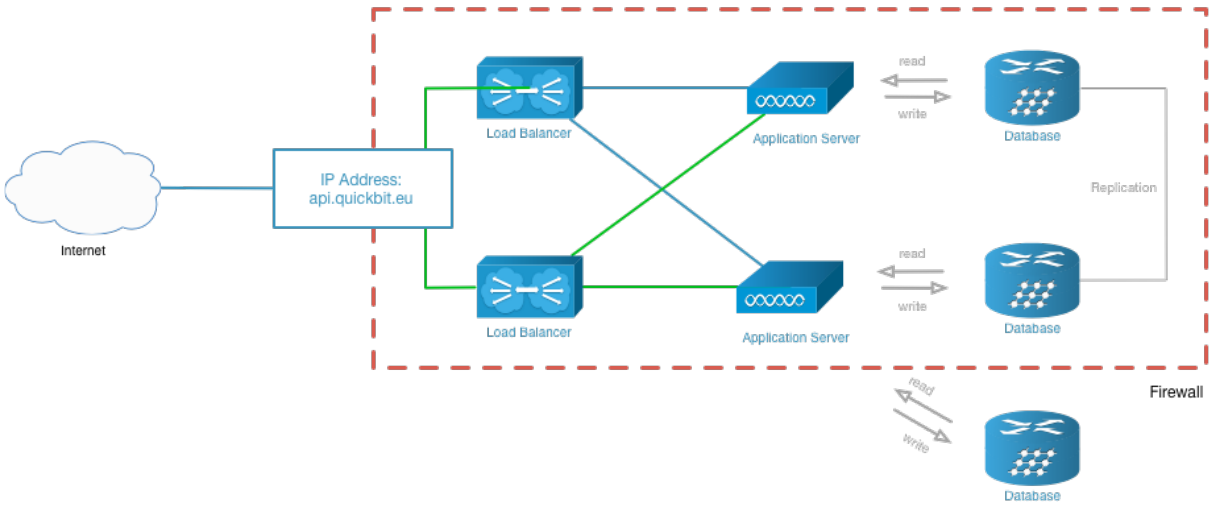
5.1 System Description

During the spring of 2019, QuickBit acquired a license to use the third-party system under its own infrastructure, enabling the QuickBit team to make rapid adaptions and implement new features without the need to rely on the third-party software vendor teams. The system is a payment gateway and payout cashier with integrated anti-fraud support.

The system is built using a *Platform as a service* (PaaS) environment which contains the full application and its underlying operating system. The QuickBit team received all the system´s source code and supporting files to install the host servers.

5.2 Systems Architecture

QuickBits system architecture is structured to handle high-volume transactions. Here security and speed are key performance criteria´s. A programming interface is accessible through the api.quickbit.eu domain address with a firewall securing the systems, databases and servers. Access is only permitted through the programming interface. See below illustration.



QuickBit follows the PCI Security Standards Council´s recommendation for data protection in how data is stored in our systems Payment card information systems, for example, always using truncated payment card information. The inventory of cryptocurrencies is stored on secure wallets with offline access, where security procedures for access involves manual action by QuickBit staff.

(

5.3 Third-party system location during data incident

The system source code was delivered to QuickBit on June 16th 2019. As can be seen in the illustration above (5.2), the third-party system and database was located outside of the firewall during the delivery and incident period. This means it was accessible with a search on the Internet.

As a part of the server setup procedure, the systems database was populated with data records by the installing engineers. This population was mistakenly made with live production data records.

Once testing was completed and the system delivery was accepted, the server was moved into QuickBit´s production environment behind the corporate firewall on July 3rd 2019.

The database was indexed by Shodan on June 28th 2019, while exposed outside the firewall. The search engine used, Shodan, crawls the Internet just like Google, and occasionally it will index things after doing IP address and port crawls, to see what's out there. This is not particularly malicious or suspicious. All search engines come across data that may have been meant to be private, but for a period of time the new system was not secured appropriately.

(

6. Exposed Data

6.1 Data fields in the database

The information for each transaction in the database included the following:

- Full name
- Full address
- Email address
- Gender
- Pro level (Gold, Silver, or Bronze)
- Date of birth
- Payment information (type of credit card used and first six and last four digits of cards numbers)
- Source currency and target currency
- Transaction amount

6.2 Size of database

The database held 301 398 data events. This was a subset of a particular e-merchant transaction flow of QuickBits transaction data for the exposed time period. The transaction flow in its entirety contains millions of transactions. No other parts of QuickBits production database was on this server.

6.3 Customers affected

17 060 customers from 50 countries were exposed. This is approximately 2% of QuickBits total number of customers. Of these 17 060 exposed, a limited number (223 customers) were from European Union countries.

(

7. Data protection concerns

7.1 Location of customers

The customer data which was exposed was from customers located in 50 different countries across the world.

Data protection legislation varies between countries. In the European Union, we have the General Data Protection Regulation (GDPR) which is in force since May 25th 2018. Other international jurisdictions have similar legislation.

223 of the affected customers are located in United Kingdom, Spain, Sweden, Germany, Belgium, Austria, Estonia, Portugal, Netherlands, Denmark, Norway, Finland, Slovakia, Poland, France, Slovenia, Lithuania, Italy, Malta, Hungary, Ireland and Latvia, within the European Union.

7.2 Legal location of QuickBit

QuickBit Limited operates as a 100% owned subsidiary with the parent company QuickBit eu AB (publ) in Sweden with head office functions. The 100% owned subsidiary QuickBit Limited operates in Gibraltar and performs daily business operations.

The Company has this structure, due to the QuickBits investors and founders being Swedish, whilst Gibraltar has pioneered legislation regarding blockchain and crypto-currencies, and it is important for QuickBit to operate within a known set of regulations.

7.3 Actions by QuickBit regarding data protection concerns

Based on the results of our internal investigation, we are in the process of contacting the affected customers to let them know about the incident, and we are reporting the incident to the Swedish Data Protection Authority and the relevant parties in Gibraltar.

(

8. Actions undertaken by QuickBit to ensure cybersecurity

We are reviewing our internal protocols and procedures to prevent this incident, or similar, from happening again. Data security is of utmost importance for QuickBit and security is one of our most important aspects of business.

The details of protocols reviewed and actions which have been taken or are to be taken cannot be made public, for the simple reason that external know-how in this field would by itself jeopardize our security.

It is important for us to state that both internal and external expertise, as well as executive management and experts from our third-party software vendor have been and are involved in ensuring the utmost data security for QuickBits system environment.

As part of our improved security procedures, QuickBit is in the process of establishing a "*Security Change Control Board*" with relevant subject-matter experts to evaluate, authorise, record and execute all changes to our security infrastructure and policies.

This will give us the confidence that oversight and good governance are in place and prevent inadvertent data loss, follow best-practice and safeguard our infrastructure from external ingress.

(

9. Författare och kontaktinformation	
Företagsnamn	QuickBit eu AB (publ)
Dokumenttitel	Data Exposure Incident Report
Datum	Friday, July 26, 2019
Författare	Chief Technology Officer
Kontakt för frågor om denna rapport	Verkställande direktör Jörgen Eriksson E-mail: jorgen.eriksson@quickbit.eu Telefon: 0046-70-681 2777

(

10. Sammanfattning

10.1 QuickBit eu AB (publ)

QuickBit eu AB (publ) ("QuickBit") är ett svenskt finansiellt teknikföretag med affärsverksamhet belägen i Gibraltar. Företaget tillhandahåller e-handlare internationellt med teknologilösningar för blockchain och kryptovaluta. QuickBit är ett publikt företag noterat på NGM Nordic MTF-marknaden.

Som en del av företagets kundlösningar upprätthåller QuickBit ett varulager kryptovaluta i Bitcoin, Bitcoincash och Litecoin och säljer till privatpersoner internationellt från eget lager.

10.2 Incident med exponering av data

Måndag 15 juli 2019 blev QuickBit informerad om en sårbarhet på en av företagets servrar. Servern var utanför företagets brandvägg och gjorde en intern databas tillgänglig och synlig för sökning på Internet.

Servern innehöll ett system som hade levererats i källkodformat av en tredjepartsleverantör av mjukvarulösningar. Medan QuickBits tekniker initierade server, installerade och kompilerade källkod, startade databas och tjänster och initiering systemet, så gjordes detta på en virtuell server utanför produktionsmiljöns brandvägg.

Därefter var databasen för teständamål felaktigt populerad med en begränsad delmängd av data från produktionsmiljön. Den exponerade databasen innehöll register som QuickBit lagrar som en del av den pågående affärsverksamheten.

301 398 datahändelser exponerades, relaterade till 17 060 kunder från 50 länder. Detta betyder inte att ett sådant stort antal transaktioner har exponerats. Ett antal datahändelser i kombination utgör en transaktion, eller försök till transaktion som kan godkännas eller avvisas av säkerhetsskäl, av identifierat bedrägeriförsök eller helt enkelt inkomplett information från kunden.

Sammantaget exponerades data för cirka 2% av QuickBits kunder. Av dessa 17 060 exponerade var ett begränsat antal (223 kunder) från EU-länder.

(

Den exponerade servern startades på QuickBits värdplattform i Nederländerna den 16 juni 2019 och den flyttades in i QuickBits brandväggsskyddade produktionsmiljö den 3 juli 2019. Detta innebär att informationen var öppen för åtkomst över Internet i 17 dagar.

Exponeringen upptäcktes och dokumenterades av säkerhetsforskaren Bob Diachenko och redaktör Paul Bischoff på Comparitech Limited i Storbritannien och QuickBit blev informerad om exponeringen via e-post från James Agate, hos Comparitech.

Exponeringen upphörde efter att den nya servern flyttades in bakom företagets brandvägg den 3 juli. Vid den tidpunkt då QuickBit blev medveten om exponeringen vidtogs omedelbara åtgärder för att säkerställa att alla servrar och databaser var säkra, innan en utredning inleddes. Utredningen har genomförts av QuickBit och systemleverantören och publika delar är dokumenterade i denna offentliga incidentrapport.

Det finns inga belägg för att någon annan än Comparitech har kommit åt databasen. Det vill säga att det föreligger inget missbruk eller försök att använda informationen som exponerats i denna incident.

De exponerade databasposterna innehöll information om enskilda transaktioner som genomförs över QuickBits plattform, och inkluderar kunds namn, adress, e-post, kön, födelsedatum, betalningsinformation (typ av kreditkort som används och första sex och sista fyra siffrorna), källvaluta och målvaluta (till exempel EUR till BTC) och transaktionsbelopp.

Varken företaget eller dess kunder har lidit eller kan förväntas lida någon ekonomisk förlust.

Den exponerade databasen innehöll inga lösenord eller nycklar till någon wallet för kryptovaluta.

Baserat på resultaten från vår interna utredning håller vi på med att kontakta berörda kunder med information om händelsen. Vi rapporterar också händelsen till den svenska Datainspektionen och till berörda parter i Gibraltar.

QuickBit beklagar att denna händelse inträffade och ber om ursäkt för bekymmer eller oro som händelsen kan ha orsakat våra kunder. QuickBit har en ambition att tillhandahålla effektiva och säkra tjänster, medan skydd av

(

personlig kundinformation är ett centralt fokus. Vi granskar nu våra interna protokoll och förfaranden för att förhindra att detta skall kunna hända igen.

(

11. Klassificering av incidenten

11.1 Överträdelse eller incident

Undersökningen som dokumenterats i denna rapport drar slutsatsen att QuickBit har varit offer för en incident.

Inom datasäkerhetsområdet används termen *överträdelse* för att beskriva förlust av kontroll, kompromiss, obehörigt avslöjande, obehörigt förvärv, obehörig åtkomst eller någon liknande term som hänvisar till situationer där andra än auktoriserade användare och för ett annat än auktoriserat ändamål har tillgång till eller potentiell tillgång till konfidentiell information. Detta har alltså inte inträffat i detta fall.

Incident är en bredare term som beskriver en händelse som faktiskt eller potentiellt äventyrar sekretess, integritet eller tillgänglighet för ett system eller den information som lagras på eller överförs av system.

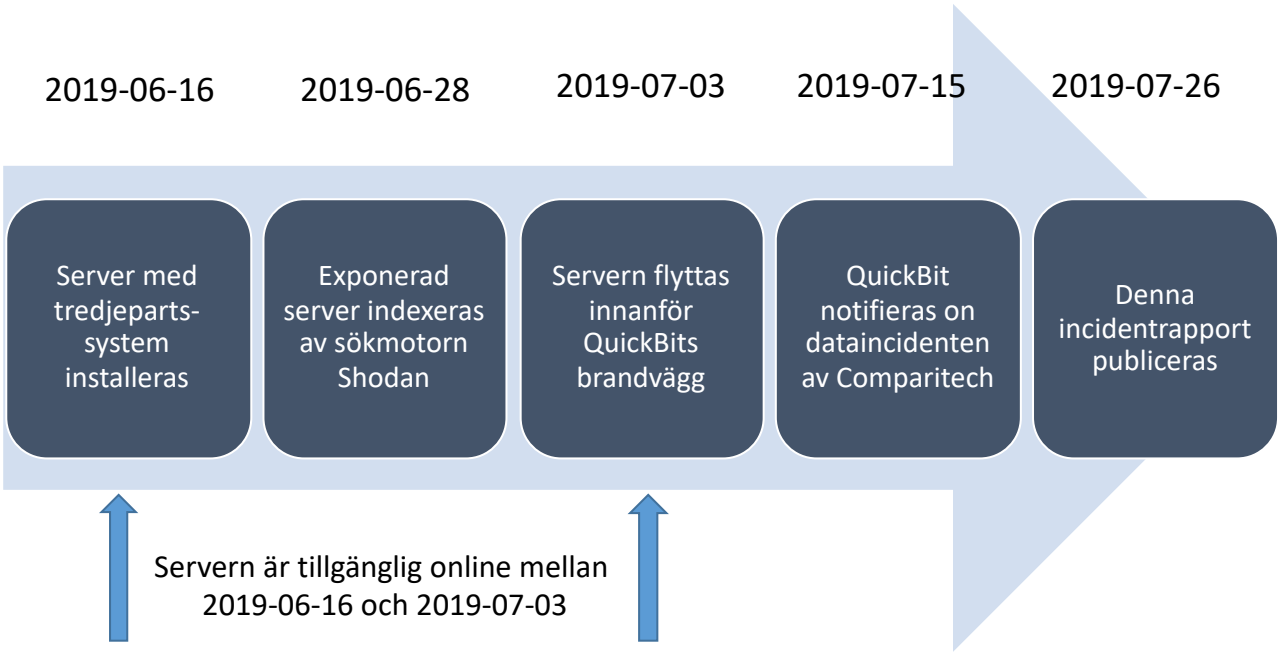
Överträdelse är en smalare term som beskriver den faktiska förlusten av kontroll, kompromiss, obehörig avslöjande, obehörig förvärv eller obehörig tillgång till information.

Den dataexponering som dokumenterats i denna rapport öppnade för konfidentiella data att vara åtkomliga utanför QuickBits-brandvägg under en period av 17 dagar. Enligt vår undersökning så var det dock endast de säkerhetsexperter som kontaktade QuickBit för att meddela oss om exponeringen som också tog sig åtkomst till data, och uppgifterna har inte spridits ytterligare eller använts för något bedrägligt syfte.

Säkerhetsexperterna kontaktade QuickBit den 2 juli 2019. Detta e-mail uppmärksammades dock inte av QuickBit, eftersom detta första e-postmeddelande bedömdes som skräppost av vår mailserver och därför inte lästes av någon på QuickBit.

E-postmeddelandet som skickades till QuickBit: s VD den 15 juli noterades dock, och Bolaget agerade då omedelbart.

12. Tidslinje



Comparitech skrev ett e-postmeddelande till QuickBit den 2 juli, men detta första e-postmeddelande uppmärksammades inte eftersom det fångades av spamfiltret i QuickBits mailserver.

Det nya e-postmeddelande som skickades från Comparitech den 15 juli till QuickBits verkställande direktör noterades och Bolaget agerade då omedelbart. Då var dock servern redan säker, eftersom den flyttades innanför brandväggen den 3 juli.

(

13. System och arkitektur

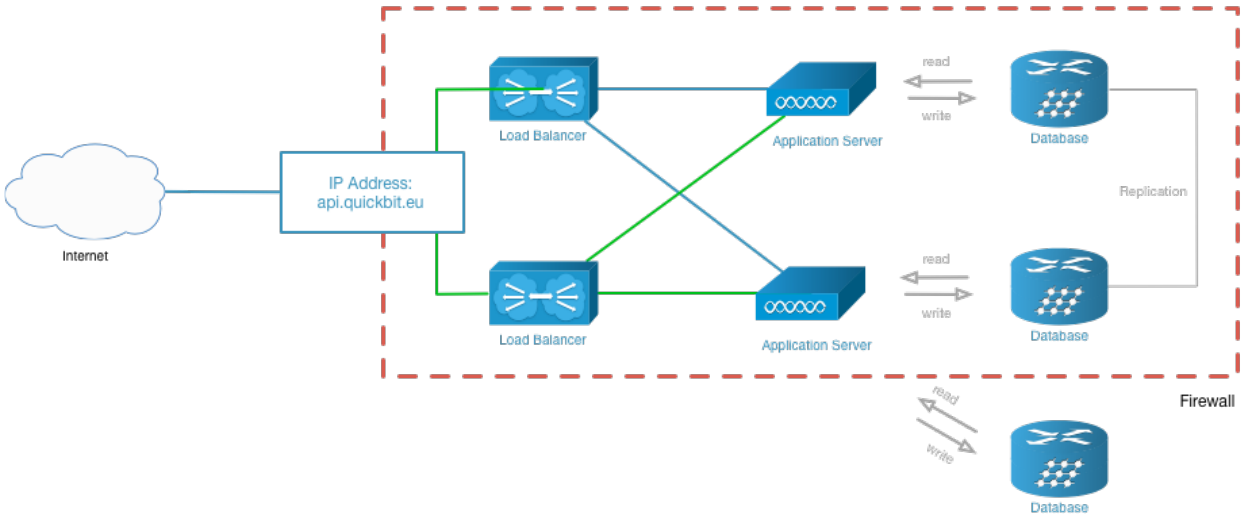
13.1 Systembeskrivning

Under våren 2019 tecknade QuickBit en licens för att använda tredjepartssystemet inom QuickBits egen infrastruktur, vilket gör det möjligt för QuickBit-teamet att göra snabba anpassningar och implementera nya funktioner utan att behöva lita på tredjepartsleverantörens kapacitet att göra ändringar. Systemet är en *payment gateway* och *payout cashier* med integrerat stöd för avancerad bedrägerikontroll.

Systemet är byggt med en *Platform as a service* (PaaS) -miljö som innehåller hela applikationen och dess underliggande operativsystem. QuickBit-teamet fick alla systemets källkod och stödfiler för att installera servern.

13.2 Systemarkitektur

QuickBits-systemarkitektur är strukturerad för att hantera transaktioner med hög volym. Här är säkerhet och hastighet viktiga prestandakriterier. Ett programmeringsgränssnitt är tillgängligt via domänadressen api.quickbit.eu med en brandvägg som säkrar system, databaser och servrar. Åtkomst är endast tillåtet via ett programmeringsgränssnitt. Se illustration här nedan.



QuickBit följer *PCI Security Standards Councils* rekommendationer för dataskydd i hur data lagras i våra system. Vi sparar, till exempel, alltid information om betalkort i avkortad form.

QuickBits lager av kryptovaluta förvaras i säkra plånböcker med offline-åtkomst, där säkerhetsförfaranden för åtkomst kräver manuell åtgärd av QuickBits personal.

(

13.3 Tredjepartssystemets lokalisering under incidenten

Systemkällkoden levererades till QuickBit den 16 juni 2019. Som framgår av bilden ovan (13.2), var tredjepartssystemet och databasen placerad utanför brandväggen under leverans- och incidentperioden. Det betyder att det var tillgängligt med en sökning på Internet.

Som en del av tester vid installationen av servern så populerades databasen med dataposter. Detta gjordes felaktigt med produktionsdata.

När tester var klara och systemleveransen accepterad så flyttades servern till QuickBits produktionsmiljö bakom företagets brandvägg den 3 juli 2019.

Databasen indexerades av Shodan den 28 juni 2019, medan den var exponerad utanför brandväggen. Den sökmotor som använts, Shodan, genomsöker Internet precis som Google, och indexerar data efter att ha gjort IP-adress och portsökningar, för att se vad som finns ute på Internet. Detta är igen direkt skadlig eller misstänkt aktivitet. Alla sökmotorer påträffar data som avses vara privat, men under en tid var det nya systemet inte säkrat på därför nödvändigt sätt.

(

14. Exponerad data

14.1 Datafält i databasen

Informationen för varje transaktion i databasen inkluderade följande:

- Fullständigt namn
- Hela adressen
- E-postadress
- Kön
- Pro-nivå (guld, silver eller brons)
- Födelsedatum
- Betalningsinformation (typ av kreditkort som används och första sex och sista fyra siffrorna i kortnumret)
- Källvaluta och målvaluta
- Transaktionsbelopp

14.2 Databasens storlek

Databasen innehöll 301 398 datahändelser. Detta var en delmängd av ett e-handelsflöde av QuickBits transaktionsdata för den exponerade tidsperioden. QuickBits totala transaktionsflöde innehåller för samma period åtskilliga miljoner transaktioner. Inga andra delar av QuickBits produktionsdatabas fanns på den här servern.

14.3 Berörda kunder

17 060 kunder från 50 länder exponerades. Det är ungefär 2% av QuickBits totala antal kunder. Av dessa 17 060 exponerade var ett begränsat antal (223 kunder) från EU-länder.

(

15. Dataskyddsaspekter

15.1 Kunders lokalisering

Den kunddata som exponerades kommer från kunder i 50 olika länder över hela världen.

Lagstiftningen om dataskydd varierar mellan länder. I Europeiska unionen har vi den allmänna dataskyddsförordningen (GDPR) som är i kraft sedan 25 maj 2018. Andra internationella jurisdiktioner har liknande lagstiftning.

223 av de drabbade kunderna finns i Storbritannien, Spanien, Sverige, Tyskland, Belgien, Österrike, Estland, Portugal, Nederländerna, Danmark, Norge, Finland, Slovakien, Polen, Frankrike, Slovenien, Litauen, Italien, Malta, Ungern, Irland och Lettland inom Europeiska unionen.

15.2 QuickBits legala hemvist

QuickBit Limited verkar som ett 100% ägt dotterbolag till moderbolaget QuickBit eu AB (publ) i Sverige som har huvudkontorsfunktioner. Det 100% ägda dotterbolaget QuickBit Limited är verksamt i Gibraltar och bedriver daglig affärsverksamhet.

QuickBit har denna koncernstruktur, på grund av att QuickBits-investerare och grundare är svenskar, medan Gibraltar som jurisdiktion har varit pionjär inom lagstiftningen om blockchain och kryptovalutor, och det är viktigt för QuickBit att verka inom kända regelverk.

15.3 QuickBit åtgärder utifrån regelverken

Baserat på resultaten från vår interna utredning håller vi på att kontakta drabbade kunder för att informera dem om händelsen, och vi rapporterar händelsen till Datainspektionen i Sverige och berörda parter i Gibraltar.

16. QuickBits åtgärder för att säkerställa dataskydd

Vi granskar våra interna protokoll och förfaranden för att förhindra att denna incident eller liknande inträffar igen. Datasäkerhet är av största vikt för QuickBit och en av våra viktigaste aspekter i verksamheten.

Detaljerad information om de granskade protokollen och åtgärder som har vidtagits eller kommer att vidtagas kan inte offentliggöras, av det enkla skälet att extern kunskap på detta område i sig skulle äventyra vår säkerhet.

Det är dock viktigt för oss att säga att både intern och extern expertis, såväl som verkställande ledning och experter från vår tredjepartsleverantör har varit och är involverade i att säkerställa största möjliga datasäkerhet för QuickBits systemmiljö.

Som en del av våra förbättrade säkerhetsförfaranden håller QuickBit på att inrätta ett "*Security Change Control Board*" med relevanta ämnesexperter för att utvärdera, auktorisera, registrera och utföra alla ändringar i vår säkerhetsinfrastruktur och policies.

Detta kommer att ge oss förtroende för att tillsyn och säkra protokoll finns på plats och förhindra oavsiktlig dataförlust, följa bästa praxis och skydda vår infrastruktur från framtida försök till externt intrång.