

Dear Sir or Madam,

Please find the answers to your questions below:

"1- Was the information of "ByLock" users requested by the Turkish government from your company?"

Please, do not confuse Cherry Servers/Baltic Servers with ByLock App authors as we have nothing in common. ByLock App authors were nothing but a one of many of our clients renting bare-metal servers for their needs.

So no, none of the Turkish government institutions has ever requested any information on any of our clients' data. Even if they would, they would have been rejected as according to Lithuanian legislation we can only reveal such data to national law enforcement institutions and only when they provide a Lithuanian court warrant.

"2- If so, what did your company reply to that formal request?"

Please, see answer #1.

"3- If not, did your main server hacked illegally by hackers? Do you have information about who the hackers are?"

We shall presume that by mentioning "your main server" you actually mean ByLock App's server(s).

We sell IaaS only. That means, that once our clients buy a server, they store their data on it and are solely responsible for the security of their data. We do not monitor it, nor we have access to it and unless clients inform us, we do not know whether or not they have been hacked.

"4- If such an illegal hacking event existed, which legal remedies has your company appealed to?"

Please, see answer #3.

"5- If the Bylock App. LOGs in your main server were not hacked by the Turkish Intelligence Agency, what do you think about how did they obtain alleged huge system data? Has your company had any idea about this issue?"

We have no speculations on this matter. The authors of ByLock App would be in a better position to answer your question.

"6- Did you investigate your firm's and employee's system LOGs whether any illegal access to the ByLock server was occurred?"

When requests like this started pouring in at the end of March 2017, for the sake of interest we skimmed through our own records and found nothing suspicious. Please note, that these records only cover physical access to the data center and infrastructure as we have no other kind of access to clients' servers (see answer #3).

"7- Is it possible that the LOGs belonging to the Bylock app. and/or a copy of whole server system content were sold to the Turkish Intelligence Agency by any of your employees without permission of your company?"

Very doubtful.

"8- In order to legalise their applications, Turkish Intelligence Agency offered to the Turkish Courts decisions taken by relevant court in the past about the purchase of LOG records and/or whole server system content from your company. What is your answer in this regard?"

This is not true. This kind of activity would be considered illegal according to Lithuanian legislation, please see answer #1.

Sevgili Bay veya Bayan,

Lütfen aşağıdaki soruların cevaplarını bulun:

"1- Türk hükümetinin" ByLock "kullanıcılarının bilgileri şirketinizden mi alındı?"

Lütfen, Cherry Sunucular / Baltic Server'ları ByLock App yazarlarıyla karıştırmayın, ortak hiçbir şeyimiz yok. ByLock App yazarları, bir çok müşterimizden, ihtiyaçları için çıplak metal sunucu kiralayan bir şey değildi.

Yani hayır, Türk hükümet kurumlarından hiçbiri, müşterilerimizin verilerinin hiçbiriyle ilgili bilgi istemedi. Onlar olsalar bile, Litvanya yasalarına göre reddedileceklerdi, bu verileri sadece ulusal yasa uygulama kurumlarına ve sadece Litvanya mahkeme emri verdiklerine açıklayabiliyoruz.

"2- Öyleyse, şirketiniz bu resmi talebe cevap verdi?"

Lütfen cevapla # 1'e bakın.

"3- Eğer olmasaydı, ana sunucunuz hackerlar tarafından yasadışı olarak hacklendi mi? Korsanların kim olduğu hakkında bilginiz var mı?"

"Ana sunucunuzu" belirterek, aslında ByLock Uygulamasının sunucularını kastediyorsunuz.

Sadece IaaS satıyoruz. Yani, müşterilerimiz bir sunucu satın aldıklarında, verilerini saklarlar ve kendi verilerinin güvenliğinden yalnızca kendileri sorumludurlar. Onu izlemiyoruz, ne de ona erişebiliyoruz ve müşteriler bizi bilgilendirmedikçe, saldırıya uğrayıp uğramadıklarını bilmiyoruz.

"4- Böyle bir yasadışı korsanlık olayı yaşanır, şirketiniz hangi hukuki yollara başvurur?"

Lütfen cevap 3'e bakın.

"5- Ana Kilit Sunucunuzdaki Bylock Uygulaması LOG'ları Türk İstihbarat Teşkilatı tarafından hacklenmemiş olsaydı, ne kadar büyük sistem verilerinin elde edildiği konusunda ne düşünüyorsunuz? Şirketinizin bu konu hakkında herhangi bir fikri vardı?"

Bu konuda hiçbir spekülasyonumuz yok. ByLock App yazarları sorunuzu cevaplamak için daha iyi bir konumda olurdu.

"6- Bayi sunucusuna herhangi bir yasadışı erişimin gerçekleşip gerçekleşmediğini şirketinizin ve çalışanınızın sistem LOG'lerini araştırdınız mı?"

Bu gibi talepler Mart 2017'nin sonunda boşalmaya başladığında, ilgi çekmek için kendi kayıtlarımızda kaydım ve şüpheli bir şey bulamadık. Unutmayın ki, bu kayıtlar yalnızca, istemcilerin sunucularına başka türlü erişimimiz olmadığı için veri merkezine ve altyapıya fiziksel erişimi kapsamaktadır (bkz. Cevap # 3).

"7- Bylock uygulamasına ait olan LOG'ların ve / veya tüm sunucu sistem içeriğinin bir kopyasının şirketinizden izin almadan herhangi bir çalışan tarafından Türk İstihbarat Teşkilatına satılması mümkün müdür?"

Çok şüpheli.

8- İstihbarat uygulamalarını yasallaştırmak için, Türk İstihbarat Kurumu, geçmiş dönemlerde ilgili mahkeme tarafından, LOG kayıtlarının ve / veya tüm sunucu sistemi içeriklerinin satın alınmasıyla ilgili olarak alınan Türk Mahkemelerinin kararlarına teklifte bulundu. ?" Bu doğru değil. Bu tür faaliyetler Litvanya mevzuatına göre yasa dışı kabul edilir, lütfen cevap # 1'e bakınız.