DELL Technologies

Lessons from a Ransomware Attack

on Universitat Autònoma de Barcelona

Gonçal Badenes
CIO, Universitat Autònoma de Barcelona.
Interview condensed and edited for clarity.

Swift action, transparency, and a renewed commitment to updating cybersecurity defined the University's response to a ransomware attack.

Sameer Shah, Dell Technologies Cybersecurity Marketing, talked to CIO Gonçal Badenes about the incident.

Shah: We've been talking about the need to help organizations incrementally improve their cybersecurity maturity. You all suffered a cyberattack some time ago. Before we dive into more detail about the attack, can you tell us a little bit the University and its IT environment?

Badenes: Universitat Autònoma de Barcelona is one of the leading universities in Spain. IT supervises all the services that are needed to run the university.

Right before the attack, we had a full plan for improving our cybersecurity posture. We had deployed multi-factor authentication (MFA), but not across all services and users. Students and all IT staff already had MFA but only on the Microsoft 365 platform. Other services were not protected. The lack of universal MFA was important, as we will see later.

When did the attack occur, and what kind was it?

It was a ransomware attack that happened on a long weekend, as is usually the case. At around four o'clock in the morning, I got a call from my team saying that there were services going down like dominoes. They raised the alarm and we immediately put together the response team that we had foreseen for these cases.

How did you know it was a ransomware attack? Was there a ransom note?

There were ransom notes on the systems that were affected. But they also conducted a minor attack by running a script to encrypt computers that were online over the weekend. The impact of that was limited, and the main purpose was probably to make sure that the staff and students found out about the attack, not just the IT team.

At any point in time, did your organization consider paying the ransom?

No.

Why not?

We couldn't do it from an ethics standpoint. Fortunately we had backups in place, two copies in two different data centers on campus and a third on tape outside the organization's perimeter.

And to be clear, these backups were not a data vault, correct?

No, not at that moment, we didn't have a vault. It was a future priority, on the roadmap. But then of course, it got prioritized [after the attack].

Communications can be critical in these situations. It sounds like you got in front of the attack by communicating clearly and transparently, including with the media?

Yes, from day one. We had to be perfectly transparent and as open as possible, explaining what had happened. We were making sure that other people could prepare and learn from our experience. My guess is that some of the press actually read the ransom note and contacted the attackers because we never did. The attacker group identified themselves as the PISA (Protect Your System, Amigo) group.

Many times organizations prefer secrecy to avoid exposing their weaknesses or remediation tactics. Was that a concern?

Those are very valid concerns. But I'm pretty sure we all know that we are vulnerable. When we try to secure our home, we know that even if we buy the best possible door, if robbers really want to go for it, they will find a way to break it or find another way to come in. This is exactly the same.

There is no shame in the fact that we were attacked and had vulnerabilities. The fact that we had a very clear roadmap for protection and were still hit is important to share with people. Even if we had some very good protection, we still had vulnerabilities that could be attacked. By implementing additional steps, you can be in a much stronger position.

Tell us what you did immediately to begin addressing the problem.

We shut down the network, all the systems. We contacted the police and the regional agency for data protection, which are things that we need to do legally. And then we immediately launched two teams: forensics and recovery. We called Dell, and it was escalated immediately to top priority, and we got a really amazing team working on it nonstop. They managed to completely recover all the data on the second data domain.

So the forensics started during the recovery process?

For some of the recovery processes, we had to wait a little bit. That's why I say forensics started first. Everything was quarantined because you need to understand what happened. We had to put together another system so we could start putting things back on. We decided that even if we would take a bit longer, all the systems that would come online would have to be up to the best standards in security.

"I believe that the most important thing to consider is that there is a significant probability that sooner or later we will all suffer a cyberattack and thus we need to have a detailed mitigation and recovery plan in place."

You mentioned that MFA was only on Microsoft 365, which was part of what enabled the attack. So, is MFA now in place across the board?

The vector of attack was a user with compromised credentials who was on a team that already had MFA on Microsoft. But when the attacker tried to access the email and saw that they couldn't access it because of MFA, they continued searching. And they found out that we have a VPN, which was not protected by MFA. Once they got access through VPN, they could start surveying the network.

In a very large network like ours, they found one system that had a vulnerability and started lateral movements. So now, once we started recovering systems, we decided nothing would come online until it was protected with MFA.

If there is ONE key recommendation or piece of advice to avoid a ransomware attack you'd want to give your peers, what would it be?

It is very difficult to give a single piece of advice, but I believe that the most important thing to consider is that there is a significant probability that sooner or later we will all suffer a cyberattack and thus we need to have a detailed mitigation and recovery plan in place.

For example, it's very important to have the contacts of key partners in forensics and recovery at hand, to have a detailed and prioritized map of services with a timeline for recovery, and a well-aligned strategy with the key business units, including communication (both internal and external). And, of course, it's very important to keep users alert and trained about the techniques used by attackers.

Do you feel the strengthening of cybersecurity capability at the university has increased confidence in continuing the mission and doing all the great things that you're doing?

Absolutely. Before the attack, one of the perceptions was that any new measures to protect the system were received with a lot of questions, and concerns about whether we really need them. The fact is protection is absolutely needed, because otherwise you put your whole enterprise in danger. And of course some people still believe these measures are hampering their work. But most feel the systems are much better protected.

Thank you. Your candor and transparency is beneficial for everyone working to advance their cybersecurity maturity.