CASE STUDY

North Devon Council and Osirium PAM and EPM

How the council achieved its cyber security goals, and protected itself from the ransomware threat

OSIRIUM

northdevon COUNCIL

Council strengthens cyber resilience with proactive, diligent approach to ransomware threat

Organisation

North Devon Council's tech analyst team wanted to tackle the following problems:

- Internal and external audits highlighted some key security concerns
- The level of privileged access for IT needed to be reduced
- Satisfying demands of cyber insurance provider which insisted upon a PAM solution
- Fears over ransomware attacks – having seen other public sector bodies badly affected
- Concerns over theft of credentials
- Making third party access secure

Solution

OSIRIUM PAM

OSIRIUM EPM

The Challenge

North Devon Council provides and manages a wide range of essential services for about 98,000 people.

Its tech team were acutely aware of cyber threats, particularly a ransomware attack and the potentially devastating consequences for the organisation and the residents who rely upon it for every day.

Paul Shears, Senior Tech analyst, says: "Ransomware attacks are what keeps us awake at night. The work we're doing, bringing on board PAM and EPM, is about reducing the attack surface for ransomware attacks. There's always that concern that someone is going to get mine or my team's credentials, and once they've got our credentials, they can pretty much jump onto any server and do anything they like."

This type of cybercrime has become a major problem for organisations in the public sector.

"The trouble is we have seen so many local authorities get hit by a ransomware attack" explains Paul. "They almost get put back to the Stone Age because they've had to literally go back to pen and paper."

Yet, Paul believes, some in public sector management underestimate the severity and ramifications of an attack and may not be aware of the dangers associated with privileged accounts.

The danger posed to back-ups

How does he explain this challenge to those unaware?

Paul says: "If I as administrator click on the wrong thing, unbeknownst to me, potentially that piece of malware can do anything I can. And if I can get to any server, it can get to any server. If I can delete the backups, it can delete the backups."

Diligently seeking to provide maximum cyber protection for the council, Paul and his team instructed two security audits to take place. These probed its resilience against ransomware and other potential threats and highlighted some key problems:

- the need for secure management of privileged accounts
- risks from IT staff having too much privilege on their admin accounts
- lack of two factor authentication

Paul says: "We've always been very good at managing software outside of the IT department but not very good at doing so within IT."

Cyber insurance catalyst

A third point of scrutiny came when renewing cyber insurance.

"The cyber insurance provider specifically said we want to see that you've implemented a PAM solution," says Paul.

Insurers are increasingly strict in terms of their requirements around software and tech, as Paul discovered.

"The level of detail for what cyber insurance requires now is quite shocking," he says.

"A few years ago, you could get cyber insurance and you didn't have to give a lot of evidence as to what you did and what you didn't do.

"Now it's a lot more stringent because a lot of local authorities have been hit by ransomware attacks, and the potential is for a big pay out. So, they expect a lot more from us."

> *The level of detail for what cyber insurance requires now is quite shocking.*

Approach

Having identified PAM as a critical addition, the team looked at products from four vendors. So, why did they choose Osirium?

"With Osirium, we thought it looked like a solution that would be quite a close fit for us to work with. I also liked the approach of Osirium's EPM product because I thought that enables us to deliver bespoke applications to staff but still retain control."

After watching demos from each provider, Darren Scott, Tech Analyst, felt Osirium was the most straightforward to set up and deploy.

On cost, Paul says: "I think it is very reasonable. IT is never cheap, but Osirium was fairly favourable."

The team began setting up EPM by using Learning Mode, which Darren described as "a really good starting point" and "incredibly useful".

It detects which applications users need, without interrupting their work. Then, it uses this information to automatically create a baseline of policies, thereby reducing calls to the help desk later on.

"It's starting to build that pool of data so then we can go and create policies, which is fantastic," says Darren.

"It's a very useful feature especially for us when we're going from an unlocked desktop to a restricted desktop. It's effectively doing a large chunk of work for me right now."

Benefits

Secure credential management

When a new member joined the IT service desk team, he started from scratch with no admin permissions, operating through PAM. This helped Darren to see the early benefits, including the fact passwords can be much longer, more complex and rotated regularly.

"He's jumping on the servers, and he has no idea what the password is he's using, which I love," says Darren.

These enhancements in password management have helped to get IT team members to buy in to PAM.

Darren says: "You've only got to type in one password in the morning with the MFA. They love it. You don't need to remember eight different passwords.

"The system with the PAM console, rather than being a hindrance to a lot of people (in that I'm taking away their permissions), is making their life easier."

Paul says: "If we had to remember those passwords, that would be a nightmare. But because we're doing it through Osirium PAM, we just let Osirium manage all of that."

> *"You don't need to remember eight different passwords. They love it.*

Reaping the rewards of time-savings

Darren says Osirium's solutions have meant "small elements of time saved - which do build up."

For example, time saving has been substantial for developers when connecting to servers – a task that required remembering multiple credentials previously.

"Our developer said 'this is the best thing ever because I no longer have to remember any passwords. I can forget them all'. So, that's an instant benefit, saving him a lot of time."

He adds: "It's given those teams much more of a managed IT service then we have before."

Furthermore, managing their 100+ servers is now significantly easier and more efficient due to the ability to create labels, and then search.

Darren says: "This feature is very easy to set up and very user friendly."

Auditing server access for the development team is becoming simpler too, Paul says.

Enhanced security for third party access

The two security reviews highlighted the lack of MFA as a weakness and this was also the case for third party suppliers, who dialled in without that extra layer of protection. This was rectified with Osirium PAM.

"The suppliers don't need to know any of the system passwords now," explains Darren. "We're increasing our security for third party companies and that's got to be a good thing."

In addition, PAM's session recording function (screen and keyboard) ensures increased control over third party access.

British-based support

Osirium is the only UK-based PAM provider – a point Paul highlights as a strength: "It does make support easier - you're all in the same time zone."

The team have been happy with the customer support provided, with Osirium's Paul Jenkinson enabling them to get up to speed on deployment quickly.

When a problem related to a Windows update occurred one night, Paul and the team had it fixed the next day.

"It was brilliant to see they wanted to get it fixed quickly and it was appreciated," Darren says, adding that Paul made himself available to jump on calls whenever questions arose.

Darren was happy with the speed of deployment, saying: "The initial set up and install was great. And Paul was very good just showing us the basics and how to set everything up."

After some initial guidance, Darren says he was able to set up a new device "in seconds".

Software updates can sometimes cause a headache, but Darren found "the upgrade was simple" when he moved from an earlier version of PAM.

Conclusion

Summing up how important he believes PAM is, Paul says: “For those who aren’t as aware about PAM, I just refer them to our audit report which said it was deemed as a critical risk IT staff having admin access.”

Darren said as an experienced IT professional he was previously a cynic and wasn’t keen on the idea of having privileged access removed. But he says thanks to Osirium’s EPM and PAM solutions he changed his mind.

“It’s a lovely way of keeping all my admin access without me having any. I’ve got full admin rights without having admin rights, and I’m finding it’s simplifying the control of administrators.”

> *It’s a lovely way of keeping all my admin access without me having any.*

Summing up his view of EPM, Paul says: “I think my concern was that once you take away local admin rights from a user, you know the IT staff are going to complain. Whereas Osirium EPM allows us to give them flexibility, but in a structured way. It means we can still deliver that piece of software to the desktop. And in fact, if we want to, we can give them the ability to install it themselves.”

Darren describes PAM as a ‘fantastic’ product but it’s the combination with EPM that makes it so powerful, he says, adding the two products “cut risk in a very quick way.”

On EPM, he says: “It’s the missing link - the extra piece in between the two – that’s where I think it will be exceedingly useful. EPM is securing my device without me thinking I am losing all my privileges, it’s the catch all.”

Overall, Paul says the introduction of Osirium’s solutions has substantially increased cyber resilience and is helping to challenge what the IT team do.

He adds: “The security footprint is definitely going to be an improvement because we’re not going to install software on people’s laptops anymore.”

About Osirium

Osirium is the UK's innovator in Privileged Access Management. Founded in 2008 and with its HQ in the UK, near Reading, Osirium's management team has been helping thousands of organisations over the past 25 years protect and transform their IT security services.

The Osirium team have intelligently combined the latest generation of Cyber Security and Automation technology to create the world's first, built-for-purpose, Privileged Protection and Task Automation solution.

Tried and tested by some of the world's biggest brands and public-sector bodies, Osirium helps organisations drive down Business Risks, Operational Costs and meet IT Compliance.

OSIRIUM

Theale Court, 11-13 High Street, Theale, Reading, Berkshire, RG7 5AH
+44 (0) 118 324 2444, info@osirium.com, www.osirium.com