CASE STUDY
CYBER SECURITY
2020

Surviving a shocking ransomware attack

Lessons from the City of Onkaparinga

In late 2019, South Australia's City of Onkaparinga was paralysed in a targeted, high impact ransomware attack. With a workforce of 700+ staff, employees that rely on technology to carry out their work were unable to do so, requiring alternative service delivery methods.

Some staff had to be sent home. Lost productivity, unbudgeted costs, immense stress & a very steep learning curve characterised the three month recovery process. Here, the Council generously shares its experiences of a total ICT shutdown and of working with CompNow & Sophos to deal with one of the world's Top 3 most dangerous hacker groups.

CITY OF ONKAPARINGA

On the southern fringe of Adelaide, the City of Onkaparinga is South Australia's largest metropolitan council. It is one of the state's fastest growing areas and the Council's staff support 170,000 residents as well as a diverse range of commercial and agricultural sector ratepayers.

THE CHALLENGE

The first obvious signs of the cyber attack appeared on Saturday 14 December 2019 when the Council's email system shut down. The incident rapidly escalated to impact every other system. There was a complete server outage, limited end user computing capacity and no access to VoIP phones. It was not only the Council's central operations that were hit but all of the community services such as libraries and support hubs throughout the 518 km² of City of Onkaparinga's suburban and rural areas.

Investigations identified the RYUK cryptolocker virus had infiltrated its ICT environment. This particularly vicious strain of cryptolocker, originating in Russia, paralyses organisations in multi-stage incidents. RYUK monitors the host, gets into the system and lies dormant before enabling the hackers to take over administration privileges to delete and encrypt critical files. While the cyber attack took place in December, indications are that the hackers had infiltrated Onkaparinga's systems in early October. And, complicating the barrage on the

"CompNow & Sophos had the best people from Australia and around the world working all hours to help bring us safely back online. They were fully prepared and across all the issues. With their combined expertise, they've also been absolutely essential to the preparation of the incident's forensic analysis and our insurance claim."

Desma Morris
Manager ICT,
City of Onkaparinga

AT A GLANCE

City of Onkaparinga Council suffered a crippling ransomware attack and recovered via a combined rapid response effort with CompNow and Sophos. CompNow engineers were onsite immediately following the attack and helped isolate, contain, remediate and protect the Council's ICT environment using the Sophos stack.

THE CHALLENGE

The impact is profound when populations lose access to Local Government services, the engine room of our communities. The seriousness of this attack cannot be understated: the Council, CompNow and Sophos were dealing with one of the top-3 most dangerous ransomware hacker groups on the planet.

THE SOLUTION

This incident highlights the importance of understanding today's very real attack environment and selecting the right technology partners.

THE BENEFITS

- CompNow project management of technology restoration process allowed Onkaparinga team to focus on business recovery
- Post-incident technology and business environment vastly improved
- Sophos 24/7 MTR now an essential element of the Council's activated crisis prevention regime

THE PRODUCTS

- Sophos Intercept X Advanced Managed Threat Response (MTR)

SOPHOS

Council's network were two other serious threats – Emotet and TrickBot.

Rapidly evolving malware strains, such as RYUK, can break into even the most diligent organisations and security aware employees. The targeted sophistication of RYUK's Phishing campaigns deceive staff with what look like genuine internal emails.

The City of Onkaparinga ICT Team Leaders Kym Groves and Zoran Bancevic explain: "We're told the RYUK emails were addressed directly to our people, covering topics they were working on. When everything looks normal, busy people are going to click on attached documents to be actioned. And when there's no immediate system issue, no danger signals are flagged."

The initial attacks would have been short lived, perhaps only a few days, so as to not raise suspicion. As the emails were distributed throughout the organisation, its contact lists were compromised. But nothing would have registered in the sent or exchange logs. The Council's Antivirus reports may have signalled for Emotet and that the attack has been cleaned, but RYUK was still at work.

Once the RYUK activated on 14th December, Onkaparinga's ICT team spent four sleepless days and nights battling the incursion. As back ups from the Friday were reinstated, a new attack at 1.30 am each night again closed everything down.

"It was insane chaos over the first few days, however because our back up data was not encrypted, we were confident we could get systems back but we badly needed boots on the ground to help. And we didn't contemplate opening any files that may have contained a ransom demand because our backups were protected. We contacted our original anti-virus vendor and they told us they couldn't help, we were on our own. Their response was terrible," Desma Morris, Manager Information Communication Technology (ICT) says.

THE SOLUTION

On the Monday following the system shutdown, the Council's crisis management plan was enacted, CompNow was called to help restore services as soon as possible, and the Local Government Association Mutual Liability Scheme engaged to recover the costs of the outage.

"We had access to nothing and had to act fast. CompNow made the case for Sophos Intercept X Advanced Managed Threat Response (MTR). They negotiated a 90-day licence to fix the immediate issue and prove its value to us for an ongoing subscription," Morris says. As another Government Department had been subjected to a similar attack, the Sophos recommendation was confidently accepted.

"Anything less than best of breed doesn't stand a chance against these Russian hackers," Morris says. Standard managed detection and response (MDR) services stop at notifying customers of potential threats. Sophos offers the additional service step of having its response experts take targeted actions to neutralise even the most virulent attacks.

The Council, CompNow and Sophos recovery team structured the management of the project's critical tasks. Daily meetings systematically monitored all actions, assessed what had been achieved and identified any shortcomings.

From Sophos' global network of security operations centres (SOC) its cloud based software actions were initiated to remotely disrupt, contain and neutralise Onkaparinga's RYUK incursion. Conference calls between the local teams and Sophos' UK SOC shared vital visibility into the environment and the evolving solution.

The seriousness of this attack cannot be understated: the Council, CompNow and Sophos were dealing with one of the Top 3 most dangerous ransomware hacker groups on the planet. "If they target you, they will get in - unless you have specifically designed, up to the minute, 24/7 protections against these types of complex attacks," Morris says.

While the Sophos MTR team investigated the source and tendrils of the hacking, the CompNow project manager and team of three engineers were on-site at the Council until late December. The first step was to identify the priority functions for restoration. With Sophos installed on critical servers,

the vital email, finance and property systems were restored on Wednesday 18th.

"The virus hit just before we were to do our pre-Christmas pay run – the largest of the year, with all the leave entitlements. We were determined to get our staff and suppliers paid so getting Payroll & Accounts Payable up was vital," Morris says.

"On the 18th we had our first successful stop of RYUK's daily 1.30 am re-encryption. It had been a really tough time but having the extra CompNow and Sophos engineers on board took the load off our really stretched internal team. With our pay runs completed, things started to look a little brighter."

With the extra "hands" provided by CompNow for troubleshooting & technical expertise, the Onkaparinga ICT team was able to focus then on the re-imaging of the Council's entire hardware fleet.

Next to be remediated were network printing & the call centre which came back online on Christmas Eve. The remote site offices & services, plus records management, were fully re-established prior to the new year. And by early February, the last of the district's Community Centres were up.

Throughout this time critical, whole-of-organisation restoration exercise, CompNow's team set about securing as much future value as possible for the Council and improving on business-as-usual. They audited and updated the processes for managing all devices enabling the ICT team to reconfigure the network infrastructure and have the user network segregated from the server network using VLANs – the new firewalls now providing an improved ability to isolate.

With each rectification action came additional issues to be overcome: licence managers stopped working, and passwords had to be re-set for every device and app.

For staff returning to work in early January, on-site kiosks were set up to scan their laptops, external storage devices and cameras. RYUK and Bot files were found in 60 devices.

An indicator of the volume and value of recovery work, the Council's six libraries had been manually checking out books and 45,000 items had to be checked back in following the restoration of services.

THE BENEFITS

"We could have been completely overwhelmed and confused through this stressful time. Everyone had their own urgency – but we didn't have the expertise or the capacity to address all the issues at once, we had to stick to our priorities. CompNow and Sophos supported us, gave us the expert authority to work through what we needed to do. The demonstrations and forensics provided by the Sophos UK SOC were clear and extremely helpful. The CompNow/Sophos solution worked like a dream, it gave us breathing time so we could be productive," Morris says.

The recovery project has a very important measurement of success. In the continuous monitoring of the Council's environment over the three months following the breach, there is no evidence of any personal data having been accessed.

Onkaparinga converted the now proven 90-day interim Sophos licence to a 3-year contract. Sophos Intercept X is loaded on each of the Council's 131 servers and 1265 devices. It is remotely, automatically updated and managed via the cloud. And the IT team monitors activity from a central dashboard.

"It's not feasible for someone sitting in a Council IT team in Adelaide to be awake analysing and defusing the 400,000 fresh malware threats that appear everyday. Sophos is monitoring the traffic on our network and status of all devices 24/7, and can remotely isolate any infection. So we can get on with running the systems for our Council knowing they'll be up and clean when we need them," Morris says.

The City of Onkaparinga undertook a comprehensive review of the 3-month incident and recovery process. Its ICT disaster recovery plan – which will now have Sophos at its core – now ensures it can remediate and protect its business critical environment into the future.

Sophos MTR Advanced ensures cost predictability for the Council if there are future breaches as the managed service is all-inclusive, and doesn't have any per-incident related costs like other managed threat services.

"As a lesson learnt, I can't stress too highly the need to regularly test your crisis management arrangements – with your trusted partners. And you don't survive something like RYUK without the full support of your executive.

"It's also vital to quarantine the recovery team from day to day aspects of their jobs. When they're on day 3 without sleep and all the servers have crashed again, station someone at the door if you have to to stop staff wandering in asking for help with non-critical matters," Morris says.

As part of the Council's insurance claim, a forensic investigator became part of the recovery team. She says: "Having CompNow and Sophos on the calls to steer the conversation and address our priorities – while complying with the investigator's information needs - gave us a strong voice in the room".

With the advent Covid 19, Sophos is continuing to provide security peace of mind. Staff working from home, often from personal rather than Council devices, have the same enterprise level protections.

Onkaparinga benefits from the strength of the overarching Local Government South Australia Information Technology Association, of which CompNow is a committed contributor.

This involvement ensures CompNow understands the specific needs and circumstances of South Australia's councils.