Article

Sep 2024

Out of Office, Not out of Risk: Why Nearly Half of All Cyberattacks Happen After Hours

This article will explore the threat landscape of out of hours attacks and how to mitigate and create a resilient 24/7 business.



Oliver Baverstock
SOC Team Lead
Email oliver.baverstock@waterstons.com





Your organisation operates 24/7, even if you don't.

Yet, despite the continued global cyber threat, businesses leave their virtual doors open, giving cybercrime an opportunity to thrive. According to recent data, 47% of all cyberattacks on Australian businesses occur outside of our normal 9-5, a sobering reminder for consistent and proactive vigilance.

This article will explore the threat landscape of out of hours attacks and how to mitigate and create a resilient 24/7 business.

The Threat

Cybercriminals operate largely through opportunity. After a workday ends, adversaries can slip through your cracks easier. Wreaking havoc in the form of ransomware attacks, exfiltrating sensitive data or installing malicious software onto your computers entirely undetected.

Nearly 50% of all Australian businesses being targeted outside businesses hours is alarming and heavily affects SME's.

SME's make up 60% of targeted cyber-attacks in Australia.

They are attractive targets, often due to weaker cybersecurity posture and hygiene. In the 2022-23 financial year, the average cost of cybercrime for small business increased to $46,000, and for medium businesses, it increased to $97,000

However, the financial and reputational damage is felt deeply after an attack no matter how big or small the organisation.

A 24/7 SOC is Essential

This complex threat landscape requires proactivity, not reactivity.

A Security Operations Center (SOC) that provides 24/7 monitoring is no longer a luxury organisations can afford not to have- it's a necessity.

Not all SOC teams are created equal. A great SOC team will be continually and proactively scanning for suspicious activity, responding to threats in real time and work to mitigate damage before it spreads.

Having a dedicated SOC team on your side ensures protection for your organisation around the clock, 365 days a year. Ensuring no breach goes undetected.

An excellent SOC and cyber partner should also be...

- Keeping you updated on the latest threats
- Provide actionable advice for an improved cyber posture
- Provide proactive monitoring 24/7, 365 days a year
- A personalised and bespoke service based on the needs of your business
- Save you time, money and headaches through their service

The Role of SOC in an Incident

When a cyberattack does occur in your organisation, a swift and coordinated response is crucial to minimise impact. With real-time threat detection, the SOC will activate an incident response plan immediately.

Rather than waiting until the next business day to address a breach- by which time substantial damage may have already occurred, the SOC allows businesses to rest easy knowing that if there is an incident- It is responded to within minutes, if not seconds.

This level of rapid response can be the difference between minor disruption and major catastrophe.

Building Trust with Stakeholders through Proactivity

A proactive 24/7 SOC builds trust with your clients, staff and stakeholders. Cybersecurity is no longer the responsibility of one business function like your IT team.

It is a business-wide problem.

Companies who can demonstrate robust security measures are more likely to earn trust and credibility in the markets you work within.

With data security becoming an increasing factor in consumer behaviours and imminent legislations on the horizon - Utilising a SOC allows businesses to not only be protected, but act as a market differentiator.

Which Type of Organisations Should Take Advantage of a SOC?

Every organisation should take advantage of a SOC.

From healthcare, real estate, finance and other sectors. All organisations should have cyber protection for the data they hold.

Any organisation that deals with sensitive information, processes financial transactions, or is part of critical infrastructure should consider implementing a SOC.

By leveraging 24/7 monitoring and incident response, these businesses can better protect themselves against cyber threats, mitigate risks, and ensure they maintain trust with their customers and stakeholders.

In a world where cyber threats don't adhere to office hours, a 24/7 SOC is critical to safeguarding your business. By staying proactive, you not only protect sensitive data and critical infrastructure but also build trust with clients and stakeholders. Now is the time to ensure your business remains resilient, no matter the hour.

If you would like more information about our SOC, get in touch below for an obligation free vulnerability assessment.

Info@waterstons.com | + 02 9160 8430

Appendix

https://cyberwardens.com.au/media-hub/a-stressful-year-ahead-top-threats-to-australian-small-businesses-in-2024/

https://assets.kpmg.com/content/dam/kpmg/au/pdf/2023/cost-of-cyber-attacks-australia.pdf

https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/small-business-cyber-security