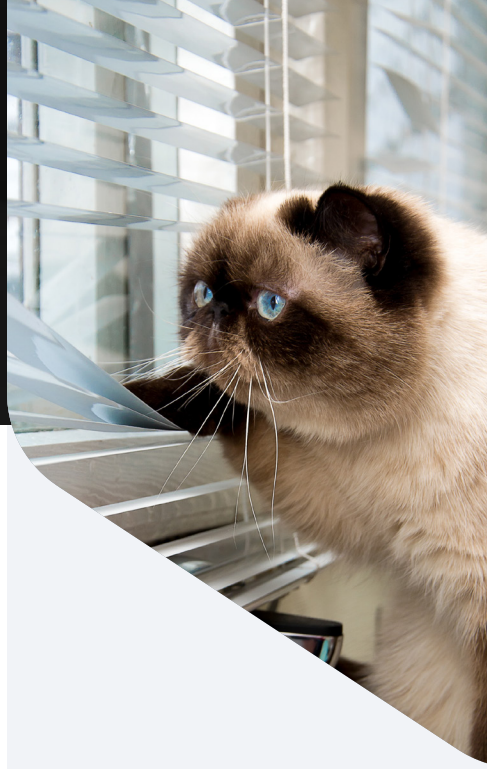
BlackBerry | CYLANCE

CASE STUDY



3 Day Blinds Takes on Cybersecurity

The Company

3 Day Blinds is an industry leader and innovator in marketing and manufacturing high quality, custom-made blinds, shades, shutters, and draperies. The California-based company has been in business since 1978 and serves clients in 5,773 cities in 25 U.S. states.

The Situation

On a sunny Los Angeles morning in December 2017, 3 Day Blinds Director of IT Operations Dan Lyle arrived at work to disquieting news. One of his network engineers had uncovered evidence that a cyber attack appeared to be underway. "I wasn't that worried at first," Lyle says now, "because our incumbent antivirus system hadn't reported anything amiss and it seemed unlikely that cyber criminals would consider us an attractive target. We don't collect masses of confidential data that cyber criminals can steal and sell for profit. We're not a high-profile multinational giant with deep pockets. At 3 Day Blinds, we market and manufacture custom window treatments. Why would a cyber criminal attack us?"

Nevertheless, Lyle recognized the critical importance of responding to a possible breach quickly, before it had a chance to spread and paralyze the company's retail and manufacturing operations. "I immediately reached out to my contacts at BlackBerry Cylance," said Lyle. A scant two hours later, members of Cylance Consulting's incident response/compromise assessment (IR/CA) team arrived on-site to begin the investigation.

The Process

According to Cylance Consulting's IR/CA team lead, "During the kickoff meeting, we introduced the teams, agreed on objectives, and compiled a detailed project plan. I explained that our methodology doesn't require us to drop hardware or software into a client's environment to collect forensic data. Often, we utilize native operating system scripts that run for five or ten minutes and then terminate, leaving no traces

Industry

- Manufacturing

Environment

- 900 Windows® desktops, laptops, and servers running Microsoft® Office and internally-developed applications
- Industrial control systems (ICS) for managing factory operations in Mexico

Challenges

- Closing gaps in the security infrastructure
- Identifying/remediating pre-existing security incidents

Solution

- Operationalizing CylancePROTECT® on all Windows endpoints
- Leveraging the best practices expertise of Cylance Consulting teams via ThreatZERO™, pen testing, and incident response/compromise assessment (IR/CA) engagements

3DAYBLINDS®
YOU'LL LOVE THE TREATMENT

behind. In this case, however, we were instructed to deploy our CylancePROTECT solution on all Windows endpoints as quickly as possible in order to detect and terminate any ongoing malware-based threats."

By the end of that first week, CylancePROTECT had flagged dozens of infected systems, confirming the initial suspicions that the company was, in fact, under attack. Given the urgency, the IR/CA team's next move was to activate CylancePROTECT's auto-quarantine mode, which promptly neutralized the malware, locked down the compromised systems, and prevented new infections from occurring. According to Lyle, "CylancePROTECT detected and stopped some very nasty executables that had sailed right through our signature-based antivirus system. Now, we needed to know exactly what had happened and how to prevent it from recurring."

Every Cylance Consulting IR/CA engagement proceeds through three distinct phases, starting with an initial assessment, followed by a targeted assessment and culminating in a forensic assessment. In the final phase, the consulting team produces a comprehensive report that documents every instance of malware, exfiltration, sabotage, command and control activity, user account exploitation, persistence mechanisms and suspect network, host, and application configurations. The report also includes risk-prioritized recommendations for preventing further incursions and strengthening the client's overall security posture.

Five weeks after the kickoff meeting, the IR/CA team formally presented its findings to 3 Day Blinds' CEO Dave Hall and the company's legal and IT management teams. "Many of the recommendations were expected," said Lyle. "We needed to decommission servers running obsolete versions of Windows, improve the efficiency of our patch management processes, and lock down administrator accounts. We were also encouraged to do a better job of training end-users to practice good cyber hygiene." By the end of the meeting, Lyle had won the executive sponsorship he would need in the coming months to put those recommendations into practice.

Accelerating Prevention with ThreatZERO Services

Not long after, Cylance Consulting's ThreatZERO services team arrived on-site and set to work completing the CylancePROTECT operationalization. Since malware prevention was already enabled, the team focused on defining, testing, and then enabling policies for script control, memory exploit protection, device control, and application control. This had the dual benefit of remediating much of the damage caused by the December attack and accelerating the company's strategic shift from a security posture of post-incident reactivity to one of proactive prevention. That milestone was achieved in March 2018.

According to Lyle, "Initially, we were concerned that implementing CylancePROTECT might overburden our IT staff or disrupt our business operations. However, the process was seamless and much easier than we expected. The ThreatZERO team also did an exceptional job of guiding and training us about security best practices. By the time they left, we were fully prepared to manage CylancePROTECT on our own."

Lyle and his team spent the next nine months implementing the security upgrades recommended by Cylance Consulting and completing other important security projects. "By the end of the year, I felt confident that our infrastructure and policies were up to par," said Lyle. To be sure, however, he decided to engage a Cylance Consulting red team for both internal and external penetration testing. That engagement kicked off in January 2019.

Red Team Rising

According to Cylance Consulting's lead red team analyst, "3 Day Blinds did an excellent job of closing the gaps we identified during our previous engagements. The environment was much more locked down than before. Still, it didn't take long for us to find significant vulnerabilities that adversaries could exploit to their advantage."

For example, threat actors often target open or poorly secured remote desktop protocol (RDP) servers because they are plentiful, easy to find, and vulnerable to brute-force password cracking. According to the lead analyst, "In this case, however, no cracking was needed because the NTFS database had been stored with reversible encryption. In about two minutes, I had the keys to the kingdom."

He also assessed the company's end-user awareness training. "I set up a server message block server to listen for connections, then sent employees an email with a weaponized embedded image and a message that read, 'How much wood would a woodchuck chuck if a woodchuck could chuck wood?' As soon as someone opened the email, it sent a request to my server to forward the employee's password hash. I was able to harvest a number of user credentials this way. Adversaries often use tricks like these to install C2 bots and other malware."

Several high-risk vulnerabilities were identified that required immediate attention. At the time, for example, 3 Day Blinds still had Microsoft's Link-Local Multicast Name Resolution (LLMNR) protocol enabled by default. This allows name resolution to be performed by hosts that share a local link. While useful, attackers can exploit this

feature by intercepting LLMNR traffic and posing as a legitimate nameserver. If successful, they can then employ a variety of methods to solicit and harvest user credentials.

“The red team’s lead analyst was extremely professional, knowledgeable, and easy to work with,” said Lyle. “We really appreciated his willingness to stop testing whenever he found a significant issue so he could inform us promptly and then assist with remediation.”

A little over a month after pen testing began, the red team formally presented its findings. “Once again, Cylance Consulting did a fantastic job for us,” says Lyle. “The report included another risk-prioritized list of security vulnerabilities and clear instructions for remediating them, which we addressed in the weeks that followed. The test results were also very reassuring, because they confirmed that the upgrades we were making to our security infrastructure and policies were proving effective.”

The Results

Since then, Lyle and his team have continued strengthening the company’s cyber defenses to stay abreast of emerging threats. “The events of December 2017 signaled a sea change in our attitudes toward cybersecurity,” says Lyle. “Previously, I couldn’t see any reason why we’d be attacked. Now, I know that attacks are inevitable, no matter who you are. I warn colleagues at other firms that their endpoints will be targeted first. If they don’t have adequate defenses, many of those attacks will get through and cause real damage. Then I urge them to follow our lead and reach out to BlackBerry Cylance.”

About BlackBerry Cylance

BlackBerry Cylance develops artificial intelligence to deliver prevention-first, predictive security products and smart, simple, secure solutions that change how organizations approach endpoint security. BlackBerry Cylance provides full-spectrum predictive threat prevention and visibility across the enterprise to combat the most notorious and advanced cybersecurity attacks, fortifying endpoints to promote security hygiene in the security operations center, throughout global networks, and even on employees’ home networks. With AI-based malware prevention, threat hunting, automated detection and response, and expert security services, BlackBerry Cylance protects the endpoint without increasing staff workload or costs.

BlackBerry CYLANCE

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

MKTG 19-0536-20190801