AUGUST 2016
www.bdo.com

AN ALERT FROM THE BDO CONSUMER BUSINESS PRACTICE

BDO KNOWS: CYBERSECURITY

ORACLE MICROS SYSTEMS DATA BREACH COMPROMISES RETAILERS' POINT-OF-SALE SYSTEMS

SUMMARY

Oracle confirmed a malware attack on its MICROS point-of-sale business via its customer support portal. Hackers with ties to the Carbanak Gang, a Russian cybercrime syndicate, used malicious code to steal MICROS customer login credentials when customers accessed the support web portal.

While investigators are still assessing the precise origin and extent of the data breach at Oracle, more than 700 internal systems have reportedly been impacted. Though payment data is encrypted in the MICROS hosted environment, that information is *not* encrypted during payment processing—when customers swipe or insert their cards. Because the main attack vector was the customer portal, and because details are still unclear, the 330,000-plus retail customers using MICROS are left to wonder about their own exposure.

Oracle's corporate network and other cloud and server offerings were not compromised, according to the company. However, Oracle is still investigating the incident and admits the extent of the damage is still unknown.

DETAILS

According to Verizon's 2016 Data Breach Investigations Report, point-of-sale (POS) intrusions are behind nearly a third (32 percent) of security incidents and *64 percent* of confirmed breaches at retailers. High-profile attacks on retailers such as Target and Home Depot underscore supply chain security risks and the potential for significant financial damage.

Hackers frequently attack third-party vendors, like payment providers, to gain access to the broader POS environment or find a backdoor entrance to a targeted corporate network. The initial attack is simply a jumping off point to get the necessary credentials to launch *another* attack on the ultimate target. In this instance, investigators believe the breach began with a single system in Oracle's network, used as a means of accessing the MICROS customer support portal, which holds information from customer support requests. Anyone who has worked with a technical support team knows that passwords, server names and other sensitive information may be included in troubleshooting documentation. This may explain why Oracle is not only forcing password resets, but also recommending that customers change the password for any account used by a MICROS representative to access their on-premises systems. This is

HOW DO I GET MORE INFORMATION?

For more information on how you can protect your business from point-of-sale system and other third-party cyber vulnerabilities, please contact:

DEENA COFFMAN
BDO Consulting Managing Director,
Technology Advisory Services
212-798-4037
dcoffman@bdo.com

NATALIE KOTLYAR
Assurance Partner, Leader of
BDO's Northeast Consumer
Business Practice
212-885-8035
nkotlyar@bdo.com

Read more ▶

a harsh reminder for IT support teams that recycle old passwords or use hard-coded login credentials why security professionals counsel against these practices.

While POS attacks have become increasingly common, the MICROS data breach is unusual in its scope and opportunity for large-scale theft. Oracle is the third-largest provider of POS software worldwide; its MICROS credit card payment systems are used at more than 330,000 terminals worldwide, including more than 200,000 food and beverage stores, and 100,000 retail sites.

If in-store payment terminals are compromised, it may explain the rash of POS attacks on retailers and hotel chains over the last few months. Further investigation will eventually shed light on how deep the data breach runs.

BDO INSIGHTS

MICROS customers aren't the only ones who should be concerned; it's an important reminder for all retailers that the new EMV chip card technology isn't a panacea. Retailers are particularly vulnerable to third-party intrusions via payment systems and other vendors, even those with seemingly innocuous access to a company's network. To address third-party cyber risk, BDO recommends the following proactive measures:

- **Establish a third-party risk management program.** All new and renewing contracts for vendors with access to a retailer's network or sensitive data should go through an evaluation process that identifies risks. The identified exposures should then be addressed with contractual provisions. The measures taken should be commensurate with the risk and the value of the contract. A creative approach rather than a single template is required.
- **Require specific protections.** Depending on the information and the circumstances, you may need to state specific data protections. Without such specification, your vendors may opt to minimize the investment in information security, exposing your company to unseen risk. And, when faced with a potential security incident, vendors that are not contractually obligated to provide timely breach notifications may leave you exposed during the weeks or months they take to investigate. Develop a written policy internally that mandates all departments entering into contracts with vendors that have network connections of any kind or receive sensitive data comply with reasonable security measures and undergo an objective, third-party security assessment at least annually.
- **Manage privileged accounts.** Many companies permit the IT department unchecked access to any and all information. These accounts should only be used when special access is required for an approved system change, and the actions taken using these accounts should be monitored even if you fully trust your IT employees. Elevated privileges are "the keys to the kingdom" and in the hands of an attacker can be used to disastrous effect.
- **Monitor for compliance.** Vendor oversight doesn't end when you sign on the dotted line. Monitor cyber readiness and potential risk throughout the third-party relationship lifecycle and set clear standards that can be subject to periodic evaluation.
- **Mandate firm-wide cyber awareness training.** On the retail floor, POS devices are exposed to temporary or seasonal employees as well as customers. Employees at every level of the company need to understand the value of the company's cyber policies and protocols and receive training on their role in preventing a security incident.
- **Develop—and test—an incident response plan.** Retailers must be prepared to respond quickly to mitigate the impact of a data breach. In addition to containing and removing the threat, the incident response plan should also take into account breach notification protocols for all stakeholders and proactive steps to minimize damage to brand reputation.

BDO assists retailers in conducting information security risk assessments, cyber risk management strategy and incident response planning, as well as breach investigations and remediation measures.

BDO'S CONSUMER BUSINESS PRACTICE

BDO has been a valued business advisor to retail and consumer product companies for 100 years. The firm works with a wide variety of retail clients, ranging from multinational Fortune 500 corporations to more entrepreneurial businesses, on myriad accounting, tax and other financial issues.

ABOUT BDO

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, advisory and consulting services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 500 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 1,408 offices in 154 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted upon without first obtaining professional advice appropriately tailored to your individual circumstances.