protiviti®
Global Business Consulting

Why you should find and close the digital gaps in your SAP landscape

There is a very good chance that your company's digital crown jewels are as vulnerable as an open backdoor in your house.

A growing number of companies face cybercrime, with considerable damage to business, customers, and reputation. And it literally happens every day. Think of the Mediamarkt, which has recently been hacked by cybercriminal gang Hive, demanding €43 million ransom. Critical internal systems didn't work. As a result, some services were no longer available to customers.

One of today's many examples showing that it can turn into a nightmare if company's 'digital crown jewels' are hijacked. Usually these are ERP-systems (Enterprise Resource Planning), that manage business critical processes and data, such as finance, operations and HR. Many companies are using the popular ERP software of SAP.

Low priority

With the current transition to a new version (SAP S/4HANA), digital safety does not get the attention it deserves, explain SAP experts Niels Willeboordse and Roy Mutsaers from consultancy company Protiviti. "Either because there are still a lot of companies using many old and vulnerable SAP versions which are difficult to patch to today's security standards, or, the pressure for the go-live with S/4HANA is very high. In the first case this means that systems are often not patched according to the latest security standards. In the second case there is no, or too little, attention for the correct "security setup" of the SAP landscapes."

Paying no or too little attention on cyber security is a long-standing problem and a risk that can no longer be ignored, as the Mediamarkt attack and many other examples show. "Security receives too little attention and priority from the organisations and apparently the implementation partners do not always point out the possible risks that may arise", says Niels. "It's not unwillingness, but rather the lack of knowledge, time and expertise within the organisations on how to effectively secure their often extensive SAP landscapes. Lots of organisations still have the assumption that they can rely on built-in security."

We would like to stretch that SAP is not secure out-of-the-box. Another issue we see is that applying patches on SAP production applications is time consuming and is often moved backwards in time due to various business reasons like unwanted

downtime or business impact. Ponemon research confirmed that it takes days, weeks or even months to shore up an application in production mode after detection of a vulnerability."[1]

Simple

How astonishing simple it sometimes is to get access, Roy regularly experiences in the 'pen tests' he runs to discover weak spots in a company's SAP security. "A client once asked us if it was possible to 'take control of the IT environment of his company,' after we found a critical vulnerability in their SAP system. Within three easy steps we were able to control the Windows domain administrator account. This means that an attacker has control over all the laptops, computers and servers that are used in the entire company. I don't have to explain the management of that company was shocked." If this had been the real deal, financial, operational, and reputational damage would be inevitable.

Being aware of the weaknesses in your company's SAP landscape is one thing, but you also need to know where to start closing the gaps. And that's where organisations get stuck, detect Niels and Roy. "You can scan the whole system and present all the results in a weighty report, but in our opinion that is only a good starting point. What we need to do next is prioritise (risk-based), starting with the basic hygiene measures like implement high priority security measures and make sure the systems are patched, and accordingly update your internal IT-controls. You can see it as closing the front door, back door and windows. After that we make a deep dive to see which other gaps need to be closed."

Security roadmap

With this so-called security roadmap Protiviti helps organisations to protect essential business applications like SAP step by step. "Some changes have a lot of impact in effort and time", says Roy. "It's important to take that into consideration and choose your priorities well informed."

And with a realistic perspective of future cyber security needs and demands. "It shouldn't be your shareholder, legislation or external regulators that forces you to be in control. You have to be convinced how important it is to protect your business critical systems on a daily basis. It is not just a one-time-effort locking the front door of your house, but you also need to make sure you have locked your backdoor and every window. That you have installed a video surveillance and that the alarm system is working."

Would you like to know more about this subject? Contact details below:

Niels Willeboordse
Associate Director
+31.20.346.0400
niels.willeboordse@protiviti.nl

Roy Mutsaers
Manager
+31.20.346.0400
roy.mutsaers@protiviti.nl

[1] www.whitesourcesoftware.com/resources/research-reports/whitesource-ponemon-research-report/