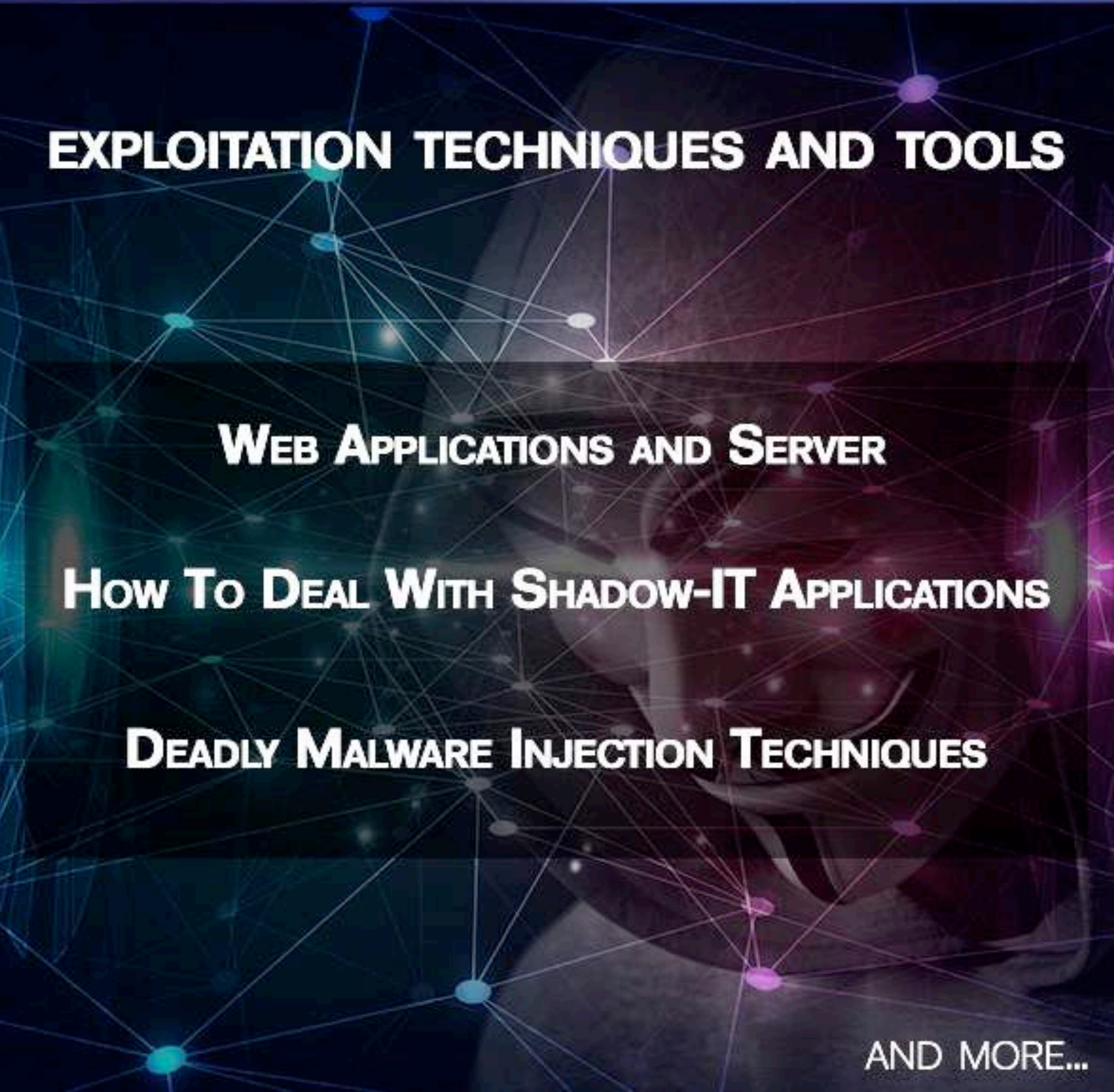
# Hakin9

PRACTICAL PROTECTION IT SECURITY MAGAZINE

VOL.12, NO. 12



## EXPLOITATION TECHNIQUES AND TOOLS

## Web Applications and Server

## How To Deal With Shadow-IT Applications

## Deadly Malware Injection Techniques

AND MORE...

# How To Deal With Shadow-IT Applications

*by Klaus Haller*

CIOs believe they control 80% of the IT expenses. In reality, they control 60%. This is the result of a 2013 study of CEB [1]. The remaining 40% represents the Shadow IT. This can be employees buying hardware such as mobile devices. It covers software developed or bought by the business. Finally, it covers software as a service, i.e. software used via the internet. In short, all IT activities outside the IT department. [2] However, the focus of this article is only the business application used to run the daily processes of the business and not provided by the IT department.

## 1. Shadow IT applications

The first category is formed by **end user programs (EUP)**, i.e., scripts or software written by end users. Some end users work in business functions and not in IT, but nevertheless have advanced IT skills. Common examples for EUPs are Excel and Access macros that automate daily routine tasks.  Second, there are **Business-operated applications (BOA)**. This is software bought and/or run by the business without involving the IT department. Third and final, there is the **Software as a service (SaaS)** concept. It is software used via the internet. A typical example is Dropbox as a cloud storage solution. SaaS is often free to use or inexpensive. Thus, SaaS infiltrates companies easily without anyone noticing.

## 2. Risks of Shadow IT Applications

This epidemic character gets obvious when googling the internet. There are tons of white papers on Shadow IT. So, Shadow IT does not only annoy CIOs. They seem to be willing to spend money for new solutions to fight the various risks of Shadow IT. They relate to governance, functional correctness, operational reliability, and compliance issues for which they might be willing to spend money.

**Compliance** is a big topic for many companies. Many companies might have to fulfill SOX or GDPR requirements or obligations set out by the FDDA. Thus, companies spend a lot of money for setting up and running huge programs with one goal: get the company and its processes compliant with such requirements. Clearly, companies do not want to spend too much on compliance and in the end, external auditors may find out about Shadow IT practices of one business team voiding all efforts and money spent.

**Governance** refers to the company rules for IT investments and budgets. They define the decision process when various project proposals compete for funding, e.g. various IT infrastructure projects as well as IT projects the business wants. Furthermore, there are guidelines from domain architects, e.g., regarding technology. Thus, a project might deliver exactly what the business team needs. At the same time, it might undermine the overall IT strategy and cause high follow-up costs others have to pay for.

In the case of EUPs, **functional correctness** is a specific risk. Not every end user can write good code plus systematic testing might not take place.

Shadow IT software poses high **operational reliability** risks. When the IT department manages an application, it ensures 7/24 support for crucial systems. They have backups in place, fail-over-systems, and business contingency plans. The support teams know the criticality of applications. They know whom to call in case of issues. Such services are unheard of in case of Shadow-IT. Thus, one business team can put a crucial process at risk. What happens if the developer of that Excel macro gets sick or leaves the company? Can a small business team manage the vendor risks if they contract with a small software vendor in a different country? What happens if a start-up goes bankrupt and the service and all data disappears overnight?

| **Application Type Risks** | **End User Programs (EUPs)** | **Business-operated Applications (BOAs)** | **Software as a Service SaaS** |
|---|---|---|---|
| *Compliance* | No integration in compliance processes | | |
| *Governance* | Governance processes circumvented | | |
| *Functional Correctness* | Code quality | n/a | n/a |
| *Operational reliability* | Not integrated in company-wide monitoring, alarming, and support | | |
| | Backup and failover responsibility of the business team | | Backup / failover functionality might not be clear |
| | Dependency of single employees | Support depends on external vendor | Dependency of business model and financial stability of the external company |

## 3. Shadow IT Applications: Managing the phenomenon

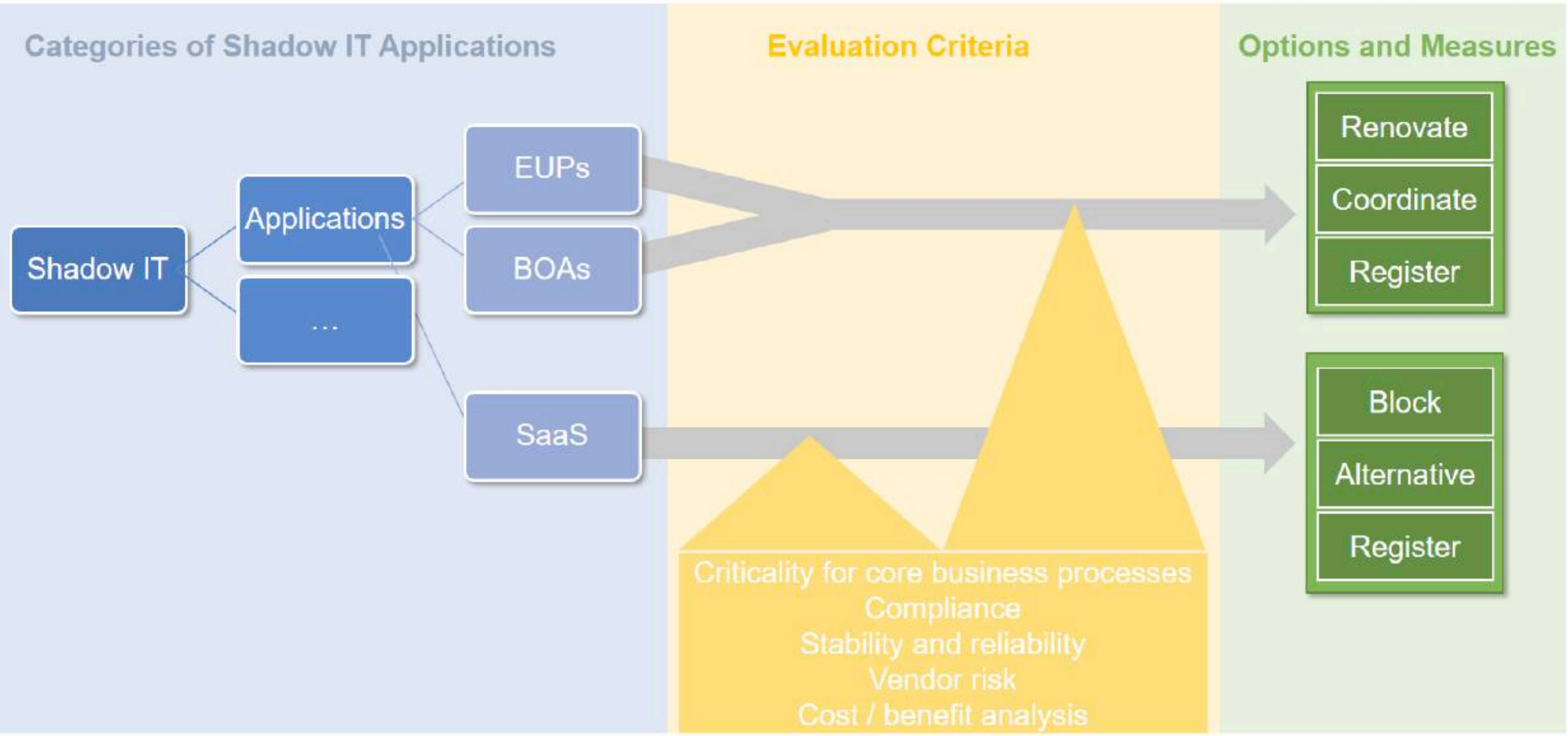
Neither ignoring the risks nor a condemnation of Shadow IT are solutions. Shadow IT can help to innovate and (temporarily) provide a quick solution for urgent business needs. Zimmermann et al. elaborated a model to categorize and manage EUPs (and BOAs) and propose three approaches [3]:

- If a software is business-critical software, but not stable and/or reliable, the IT department should take over the application and renovate it.
- In the case of non-business-critical and stable and reliable software, the EUP or BMA should be simply registered. The business remains fully responsible for its operations.
- In less clear cases, the business and IT should coordinate their activities and work together. A typical scenario is that IT takes over infrastructure related tasks. The business remains in charge for business related tasks.

This model can be extended in two directions to cope with today's needs. First, the actions to be taken for EUPs and BOAs remain the same. The decision criteria business-criticality and stability/reliability must be extended by the additional criteria vendor risk, cost/benefit analysis, and compliance.

In the case of SaaS, a different measure is that the IT department's vendor risk and operational risk management processes cover the SaaS solutions once they are registered. This can be the perfect low-effort option for non-business critical SaaS with a low risk profile.

- ➡ Provide an alternative. The IT department contracts a similar service from a service provider in a more adequate jurisdiction or with a longer successful track history in the industry. Hosting a new tool in-house is another option. This makes sense for software used in the company by many different teams.
- ➡ Register the SaaS.
- ➡ Blocking the SaaS completely. The old-days Napster would be such a service to block. This is the solution for high risk SaaS solutions for which no adequate alternative in-house or from another service provider can provide.



To conclude: Shadow IT is an epidemic phenomenon companies and IT departments have to accept as reality. It helps companies to innovate and to get more efficient. Thus, just buying software to suppress all SaaS in your company is not sufficient, because it prevents innovation and does not address EUPs and BOAs. Instead, CIOs need a strategy to manage the phenomena to benefit from its opportunities and to mitigate and reduce associated risks.

## References:

[1] Tom Groenfeldt: "40 Percent of IT Spending Is Outside CIO Control", Forbes Online Edition, December 2nd, 2013

[2] Ch. Rentrop: Shadow IT risk: empirical evidence from multiple case studies

[3] Stephan Zimmermann, et al.: Managing Shadow IT Instances - A Method to Control Autonomous IT Solutions in the Business Departments, 20th American Conference on Information Systems, Savannah, 2014