



STORMSHIELD


OPINION ARTICLE

WHY DO UPDATES POSE A PROBLEM IN THE CYBERSECURITY WORLD?

Adrien Brochot
Product Manager,
Stormshield

Ah updates... Those pesky updates, all too often labelled as “restrictive”. However, these updates exist for our own good. And although it’s often difficult to make reasonable IT security choices if these are detrimental to production, updating is something which can’t be put off until tomorrow. On the contrary, it should be a central aspect of any company’s security policy.

Why carry out updates? **Are updates absolutely vital?** Can’t they wait for a while? These questions and many others are all too frequently asked in many companies, for whom digital hygiene, IT protection and best practices in the security field aren’t always synonymous with updates. And they’re not always a priority. For companies, business continuity and production capacities remain their number one priority, with the issue of IT vulnerabilities often taking a backseat.



However, although a company's production must never be brought to a standstill, cyberattacks are not going to stop any time soon either. As long as there are vulnerabilities, there will be attacks. And the updates are needed to patch these vulnerabilities and fend off these attacks! Although their efficiency and importance are well demonstrated, the road to acculturation is a rocky and winding one. Within companies, a combination of urgent priorities and ambivalence ensure that operational requirements are always placed ahead of the fight against the cyber risks inherent to their activities.

NEGLECTED UPDATES AND VULNERABLE SYSTEMS

The bugs and vulnerabilities in question, which are documented and published by stakeholders in the cybersecurity sector, can range from minor bugs to critical vulnerabilities. And if this information is available to companies, that means the attackers also have access to it... Systems which have not been updated are therefore particularly vulnerable to cyberattacks. *"The attackers use footprinting systems, namely scans of the networks and environments enabling them to identify the machines, to easily and quickly find workstations open to attack, in this case those which have not been updated"*, explains **Guillaume Boisseau**, from Stormshield's Professional Services Department. There's no doubt that non-updated systems offer possibilities for attackers to carry out malicious acts. *"The attackers will particularly develop an in-depth attack on an IT system in the case of old systems containing vulnerabilities, which are well-known and exploited by malicious networks"*, adds **Maxime Nempont**, Technical Leader for Security at Stormshield.


When dealing with non-updated workstations, the WannaCry ransomware perfectly illustrates how vulnerable such workstations can be. In May 2017, this ransomware program was able to spread thanks to a vulnerability in Windows environments, within systems which had not patched the security flaw. However, two months before the attack, Microsoft had published a security patch for this vulnerability and issued a warning concerning its high importance. The final tally: 150 countries were paralysed by the WannaCry cyberattack and the financial losses have today been calculated into the billions of dollars.

WannaCry offers a snapshot of the reality we are still experiencing today: many companies have not yet clearly identified the vital importance of carrying out updates and of doing so as soon as possible to reduce the window of opportunity for attackers.

"Updates are a bit like your appointment at the dentist: if you have a check-up regularly, you'll only have a few minor things that need doing each time. On the other hand, if you don't go to the dentist for a long while, things accumulate and get worse."

Guillaume Boisseau, Stormshield Professional Services Department





In May 2019, Microsoft once again published details of a security flaw concerning one of its system components. Baptised “BlueKeep”, this flaw could have had the same impact as WannaCry if it had been exploited on a large-scale basis. Although for the time being cybersecurity researchers cannot confirm that BlueKeep has undergone large-scale exploitation by attackers, the risk certainly existed. Because a month after the revelation of the flaw and publication of the patch by Microsoft, almost a million systems were still exposed and vulnerable. All possible entry points to the malware ecosystem...

“Some companies don’t perform updates as they don’t have the procedures in place to provide a framework to ensure these are done properly (such as a lack of test environments for example) and so the updates accumulate, and with them the attendant risks. “It’s a bit like your appointment at the dentist: if you have a check-up regularly, you’ll only have a few minor things that need doing each time. On the other hand, if you don’t go to the dentist for a long while, things accumulate and get worse. The same pretty much applies with updates!” explains Guillaume Boisseau.


The spectre of WannaCry appears to loom large on a regular basis: this year, another major flaw linked to the Windows operating system was detected, named SMBGhost. A vulnerability in the same protocol as that used by WannaCry, the exploitation of which could have been catastrophic.

Attacks targeting non-updated systems are on the rise and won’t be stopping any time soon. Both simple to perform and well documented, they offer many benefits, of which the attackers are all too aware. **More than ever before, performing updates should therefore be considered a priority by all companies**, whatever the business sector, and should become an ingrained part of any organisation’s culture.

RECONCILING CYBERSECURITY AND IMPERATIVE OPERATIONAL REQUIREMENTS: BETWEEN THE HOLY GRAIL AND THE ETERNAL PARADOX

Updates to software, applications or devices are and will always be the subject of competing pressures, with the twofold objective of guaranteeing security and taking account of the operational constraints inherent to all activities.

Because although updates exist to squash bugs and patch critical vulnerabilities, they can also generate constraints for companies. In industry and operational networks (OT), updates are particularly unpopular as they can generate undesirable effects, such as a prolonged stoppage of production. And even once completed, restarting the system is a critical moment requiring careful attention in the industrial world. Through a rebound effect, unforeseen impacts can result in falling production, which has an adverse effect on turnover. *“Assessing the need for an update by carrying out a*



*risk analysis and planning this while measuring the impact on production are therefore imperative aspects which should be taken into account in industry”, stresses **Florian Bonnet**, Product Management Director at Stormshield. “For this reason, maintenance cycles must be carefully prepared and scheduled in the industrial world”.*

But the constraints are not only found with OT. More generally, updates can result in the company taking a step backwards, with a website becoming unavailable, or in lost time for users who find themselves obliged to restart the equipment and to cease all office software tasks for a certain time. These same updates can also entail constraints due to the components they involve and directly affect software or applications currently under development, to the great displeasure of the developers! – or applications already deployed on the workstation.

So, whether you're the head of a textile production plant, a web developer or a common mortal sat in his office, updates are not particularly welcome, and their deployment can be a source of worry and reticence. The issue of updates is therefore as complex as it is paradoxical.

THE QUESTION OF THE UPDATES' IMPACT

So, **should you or shouldn't you update?** To update or not to update? That is the question! And an important one too... According to the operational constraints and working environments (production environments, applications used, etc.), updates can prove to be very complex or even impossible. *“Some work is required ahead of an update to be able to determine whether it's likely to affect the workstation or the working environment. For sensitive environments and critical systems for example, it's necessary to envisage a pre-production environment in the event that the updates result in the system malfunctioning - or in changes to the way it works”,* explains Guillaume Boisseau.

You should adopt the principle that in the wonderful world of updates, control procedures and anticipation are the watchwords, including in the case of automatic updates (PCs, tablets, etc.) for which it's also important to be able to check reliability and limit risks. *“In IT, automatic updates can be activated for workstations or office software in as far as they can always be postponed and performed at a more convenient time”,* explains Florian Bonnet. He adds that *“for IT servers or in OT on the other hand, automated updates cannot be envisaged as these are critical systems for which the consequences of updates must be managed in detail”.*

Indeed, in some cases it's impossible to perform updates as such, as these require the deployment of high availability architecture - or even digital twins or other forms of virtualisation - to test them. In the OT field, this test environment is therefore vital to be able to assess the risks posed by an update and to avoid disrupting the operational system.

Other scenarios may make it impossible to perform updates, such as *“when an update results in an application becoming incompatible with an old operating system or in the case of systems at the end of their operational lives, for which the update and migration to the new system become excessively costly”*, explains Maxime Nempont. With this in mind, it’s not hard to imagine why companies are reluctant to perform updates rather than the reverse - despite the IT security needs. In this case, the publishers play a key role as both advisers and facilitators, to help companies perform their updates and to find a workaround solution when this is impossible. Their goal: **To develop the simplest update systems possible** and to ensure that companies can benefit from these.


But first and foremost, it’s the companies themselves who need to understand the importance of updates and their applicability. **Because failing to perform updates means leaving yourself exposed to cyberattacks**, for which vulnerable systems offer a highly-prized open door to your system.

DEVELOPING AN “UPDATE CULTURE”

Although, overall, companies are increasingly aware of the issue of updates, they may still experience difficulties in evaluating and understanding the risks of failing to implement them. Additionally, not all companies appreciate that they can be the target of a cyberattack. This is the case with OT, in which “cyberculture” is not yet widely developed. However, as Florian Bonnet reminds us, *“It’s not a question of if you’re going to be attacked but rather when”*, before adding: *“making updates part of the company culture also entails accepting the cyber ecosystem more generally as part of the company culture and then keeping up to date with the latest news...”*. Companies therefore need to become more aware of what’s at stake, and the publishers are there to help.

“It’s not a question of if you’re going to be attacked but rather when.”

‘Proof by example’ is a method which works quite well in the opinion of Maxime Nempont, who explains that *“you need to take concrete cases, and talk to people about the real-life exploitation of critical vulnerabilities, making them understand that this is not just theory”*. As well as raising awareness, the publishers should also provide support through the update process and be very precise when issuing a new patch to inform the client, who must be able to clearly understand whether this is a bug fix or a vulnerability patch. *“The publisher must ‘justify’ the updates they propose and present the associated risks to reassure the company, because one way or another the customers will always be tempted to prioritise production over everything else”*, states Guillaume Boisseau.



Clear explanations from the publishers are therefore essential for companies to take this onboard as part of their company culture, but more is required too. IT managers also play a key role as part of this process. Indeed, the updates and the related procedures (update frequency, the decision as to whether to activate automatic updates or not, etc.) are the responsibility of the IT departments and must be managed and centralised by them and not by the users. The IT teams are best placed to correctly respond to the issue of updates and to supply the right supervisory resources needed to deploy them.

But some countries have preferred more coercive measures as opposed to the simple provision of information, with an example being the United States, which adopted firm measures when faced with the recent threat of Zerologon – a security flaw affecting Windows servers within corporate networks. If exploited, this vulnerability could enable an attacker to take control of vulnerable machines, and in particular domain controllers. In such a context, the US Cybersecurity and Infrastructure Security Agency (CISA) has acted firmly: all of the country's governmental agencies must have applied the patch for this vulnerability before midnight on 21 September. To avoid such a situation coming about and to give the provision of clear information a chance of succeeding, the best solution continues to be to focus on making this part of the company culture, helping firms to understand the issue and reassuring them of their ability to remain productive while also adopting the right security measures.



STORMSHIELD

All around the world, companies, governmental institutions and defence organisations need to guarantee cybersecurity for their critical infrastructure, their sensitive data and their operational environments. Certified and qualified at the highest European levels, Stormshield's technological solutions meet the challenges faced by IT and OT to protect their activities. Our mission: to provide cyber-serenity for our clients so they can concentrate on their core activities, something which is vital to the satisfactory operation of our institutions, our economy and the services provided to our populations. When you choose Stormshield, you are choosing a trusted European cybersecurity provider. Further information: www.stormshield.com