based on their effectiveness. It is a useful technique for creating unique rules that would otherwise not be created, but it's only possible if you have all the data available at the same time, which is what graph is good at.

A big concern with automated fraud detection systems is the issue of false positives. First, it can absorb a lot of time and effort from human analysts dealing with the false positives and filtering out the hits that really need more investigation. And secondly, there is a concern about the impact on customers – as one telecoms company explained, it wants to take automated fraud detection slowly because one of its biggest fears is getting a false positive and losing a legitimate customer over it.

If you approach fraud detection with graph without sufficient preparation, you can run the risk that suddenly everything looks like fraud. However, graph feeds very well into machine learning – it is very good at generating data for training ML systems because it is very good at producing explainable models of what it has detected. Rather than simply giving something a score based on heuristics, graphing can generate data on the links between different objects in the database, which can be fed into ML systems for further analysis. This explainability extends to showing humans what's going on, as the linking data can be used to draw detailed diagrams from which humans can infer the relationships between the objects and ask further questions.

"Graph databases are good at showing results graphically, making explainability one of its key strengths. This, combined with the ability to explore contextual data, makes them an asset in fraud detection"

The region of confidence (ROC) curve tells you how confident you are in the decision that a machine made. Some decisions you can accept from the machine alone based on the score. But if your confidence is below 50-60%, and depending on the value of the transaction, you might want to forward this to a human analyst. The analyst really needs to understand why the machine thought there was a 50% chance that the transaction was bad – you don't want to force the human to go back to the beginning to work out why. You want them to take a case from the system and work it quickly and confidently with all the information to hand.

Graph databases are good at showing results graphically, making explainability one of its key strengths. This, combined with the ability to explore contextual data, makes them an asset in fraud detection. Feedback from the analysts can also be fed into ML and graph systems, creating a virtuous circle between humans and machines that can make fraud teams more efficient.

About the author

Richard Henderson is a solution architect at TigerGraph EMEA (www.TigerGraph.com). He has been an independent data system designer for over 30 years, consulting to most major industries, including FIS, banking, retail and manufacturing. For the past 10 years he has concentrated on bringing the most advanced data technologies to market, with graph analytics as the natural evolution of that journey.

References

1. 'Online Payment Fraud Losses to Exceed $200 Billion Over Next 5 Years'. Juniper Research, 25 Feb 2020. Accessed Jun 2020. www.juniperresearch.com/press/press-releases/online-payment-fraud-losses-to-exceed-200-billion.
2. 'Why Experts See Graph Databases Headed for Mainstream Use'. eWeek, 27 May 2020. Accessed Jun 2020. www.eweek.com/database/why-experts-see-graph-databases-headed-to-mainstream-use.

Overcoming the security risks of remote working


Florian Malecki

Florian Malecki, StorageCraft

The Covid-19 pandemic has transformed the way businesses operate. Around the world, governments have implemented regulation to protect people and slow the spread of the virus. This includes strict lockdown and social distancing measures that have prompted entire workforces to start working remotely.

As millions of people work from the safety of their homes, we have witnessed the creation of the largest-ever global remote workforce. IT teams have been relied upon to create work-from-home setups for entire companies. Moving millions of employees, their computers and their data away from a secure office environment presents tremendous data security risks at the best of times, let alone when the transition has had to happen in a short space of time.

With risks ranging from simple technical glitches and human error to full-

scale ransomware attacks, there is a lot at stake for businesses. The role of IT teams in business continuity has never been more important.

The new normal

It goes without saying that a major consideration for business leaders during this period should be the health and wellbeing of employees. This spans from sharing tips to help employees stay active at home, to the leadership team communicating regular business updates.

"It's imperative that all company data is backed up, protected and easily recoverable in the case of a breach. This is made more challenging by the dramatic rise of dispersed and remote users"

Aside from this, a top priority is to make sure employees have the right IT equipment and adequate connectivity to work productively and efficiently from home. This encompasses a range of factors, including the provision of laptops, keyboards and other hardware essentials, checking that workers have sufficient access to network and data and ensuring that they have secure online environments.

Employers must also take into account the heightened security risk of running a remote workforce. It's imperative that all company data is backed up, protected and easily recoverable in the case of a breach. This is made more challenging by the dramatic rise of dispersed and remote users, which creates a great many more entry points for attackers.

The cybercrime pandemic

It is a sad, yet inevitable, fact that cyber criminals are exploiting the Covid-19 pandemic by launching ransomware attacks on unprepared, unprotected businesses. From February to April 2020, amid the Covid-19 surge, cyber attacks against the financial sector increased by a staggering 238%.[1] Furthermore, those surveyed reported that attempts at destruction, not just information theft, are becoming more common.

Also concerning was 82% of CIOs reporting that, alongside a spike in attacks, the techniques used by cyber criminals also appear to be improving. Specifically, they highlighted the use of social engineering and more advanced tactics to exploit not only the human factor, but also weak links caused by processes and technologies within the supply chain.

Now more than ever, organisations that do not have the right infrastructure and policies in place to protect against malicious actors will find themselves most at risk. To mitigate this, there are a number of steps that businesses should take to safeguard data and protect the network while working remotely.

Protecting business data

A first step for any business moving to a remote working setup should be to implement a company-wide policy that automatically saves documents and data to a shared area such as Google's G Suite, Microsoft O365 or a company's own on-premises shared drive. It's important to remember that some of these hosted services only have 30-day retention for files, so businesses should add a back-up solution and match the back-up frequency to the importance of the data.

Employees working with unstructured data should be encouraged not to store their files on their own laptops, but rather to store work files on a company-managed file server that has immutable snapshots capability. This server should be protected with image-based back-up software to ensure the constant availability and recoverability of all data.

Image-based back-ups can also be used on employee laptops. This means that should an employee's laptop fail, the back-up can be used to restore the operating system, applications and data to a new laptop in minutes. Not only does this mean minimal downtime for the employee in question, it also means that any data that wasn't stored to the shared drive or cloud will also be recovered.

"Since ransomware is able to encrypt back-ups, it is recommended to go a step further and replicate the back-up images to a remote site or to the cloud. This ensures that the files are still secure and easy to recover"

Local back-up images may be sufficient to protect the data. However, since ransomware is able to encrypt back-ups, it is recommended to go a step further and replicate the back-up images to a remote site or to the cloud. This ensures that the files are still secure and easy to recover. When doing so, businesses should check that the SLA matches the importance of the data, and that the data is replicated to an offsite datacentre or a third-party cloud provider.

Having taken these steps, business leaders can be safe in the knowledge that mission-critical data and applications are fully backed up.

Secure, remote network

As well as protecting business data, there are a number of additional steps that businesses can take to build and maintain a secure remote working environment, including:

- **Safeguard infrastructure**: It's important to be confident in the knowledge that business infrastructure is protected with strong security protocols. Part of this is ensuring that all work devices have the appropriate endpoint protection measures installed and a strong VPN solution for a secure connection to the company network.
- **Secure the network:** With cyber criminals looking to exploit the

sudden surge in remote working, it's imperative that businesses take the necessary steps to secure their network. This includes the deployment of software that can constantly scan for viruses and suspicious connections.

- **Encourage employees to utilise the IT support team:** Employees should be encouraged to consult IT support teams with any concerns rather than trying to solve technical issues alone. This will ensure that issues are resolved as quickly and securely as possible and could help to avoid a bigger problem arising in the future.
- **Communicate safely:** Ensure that the tools used for company-wide communications, such as instant messaging and video conferencing, meet recognised security standards. Staying connected is essential but it shouldn't come at a cost to security.

Empowering employees

As well as deploying the correct storage infrastructure on a company-wide scale, it would be remiss for business leaders to ignore the important part that employees play in keeping the network safe. Phishing attacks that attempt to steal personal data from an email recipient, in particular, remain a concern, especially when considering that attacks rose by 600% in Q1 2020.[2] A successful phishing attack can expose a company to potentially catastrophic ransomware attacks. As well as testing the network to find any holes in protection, it's essential that businesses invest in educating employees to be able to identify and avoid phishing attacks. This is especially important when considering that human error accounts for a quarter of all data breaches.[3]

From encouraging the use of multi-factor authentication (MFA), to using strong passwords, the actions that employees take from their living rooms will have a direct impact on the security of the business. They should receive clear guidance on how to secure home routers and manage wifi access, as well as education around setting up secure domain name servers (DNS) to optimise protection against malware, phishing and ransomware.

When properly educated and well prepared, employees can prove a crucial weapon in the fight against ransomware.

Dealing with an attack

For a company to be confident in its ability to recover, it's essential that back-ups are regularly tested. Unfortunately, this is not always the case, as shown by recent StorageCraft research, which revealed that while 68% of respondents believe they have a clear plan in place and could quickly recover from a ransomware attack, 46% only test their plans once a year or less.[4] While having a back-up plan is important, being able to recover all data completely and quickly is absolutely critical for business continuity.

It's important to remember that even the best-laid plans can sometimes fail. This is where a robust data recovery plan is essential to business continuity. Being able to recover data quickly in the event of an attack ensures minimal damage and downtime, and as a result, reduces the risk of lost revenue for the business.

If the worst happens and a business does fall victim to a ransomware attack and does not have a data recovery plan in place, it is important that it keeps calm and does not pay the ransom. To pay is to encourage hackers to continue to launch attacks and is also an indicator of how vulnerable an organisation is, which can increase the likelihood of further attacks.

Expert advice should be sought where relevant – for example around any legal complexities, and customers should be informed in a targeted and co-ordinated manner to avoid panic.

Looking to the future

For many businesses around the world, it remains unclear when they will be able to return safely to an office environment. With the threat of cybercrime more prevalent than ever, now is the time for organisations to put the software, policies and tools in place to ensure business continuity and safeguard against the threat of ransomware.

About the author

Florian Malecki is international product marketing senior director at StorageCraft. He drives the development of the vendor's data protection and storage solutions. Prior to joining StorageCraft, Malecki worked in senior roles at SonicWall, Dell, Aventail, ClearSwift, Omgeo, Lucent Technologies and Air Products. He earned a master's degree in business, marketing and technology from the Ecole Supérieure Des Affaires et Des Technologies, France.

References

1. 'Modern Bank Heists 3.0'. VMWare Carbon Black. Accessed Jun 2020. www.carbonblack.com/resource/modern-bank-heists-3-0/.
2. Sjouwerman, Stu. 'Q1 2020 Coronavirus-Related Phishing Email Attacks Are Up 600%'. KnowBe4, 9 Apr 2020. Accessed Jun 2020. https://blog.knowbe4.com/q1-2020-coronavirus-related-phishing-email-attacks-are-up-600.
3. 'How much would a data breach cost your business?'. IBM. Accessed Jun 2020. www.ibm.com/security/data-breach.
4. 'StorageCraft Research Reveals Rampant Data Growth, and Inadequate IT Infrastructures Are a Source of Global Concern and Risk'. StorageCraft, 12 Sep 2019. Accessed Jun 2020. www.storagecraft.com/press-releases/storagecraft-research-reveals-rampant-data-growth-and-inadequate-it-infrastructures.