VMGROUP : INVESTIGATES

Cyber Crime 2019 – Are we really doing anything about it or pointing blame at others?

By Dr Vivienne Mee, VMGroup

www.vmgroup.ie

VMGROUP : INVESTIGATES

Cyber Crime 2019 – Are we really doing anything about it or pointing blame at others?

Cyber crime, fraud and economic crime is on the rise, with 49% of organisations reporting being victims in the past 24 hours. Why are the numbers increasing daily? Are the hackers that intelligent and are the attacks that sophisticated?

It is easy to blame the hackers or fraudsters, but have organisations started looking at their own practises to ensure they are not leaving their doors or data wide open?

VMGroup partook in their own study in 2019 to determine if organisations were looking after the basics of security and implementing best practise and procedures within their organisations.

The purpose of the study was to determine if organisations were taking their security seriously and to determine if Organisations were looking after their client's data as they should.

We all are aware now of the latest GDPR rules and regulations. A year and a half on from the enforcement of GDPR, our study highlighted that we are no better off now then we were 16 years ago.

The Study

So, our study – we repeated a study conducted in the UK as far back as 2004 – retrieval of information from hard drives readily available on the second-hand market. Dr Vivienne Mee, CEO and Founder of VMGroup, partook in this study in 2004 alongside fellow researchers at the University of Glamorgan. The Information Security Research Group at Glamorgan caused a stir back then, and this continued for the following years.

The purpose of the VMGroup team revisiting the study was to determine if any information could be retrieved from these drives and devices. It was a bonus if we could identify individuals, organisations or charities.

The results in 2004 and subsequent years were alarming and everyone commented on how stricter rules should be enforced and more security standards should be aligned.

The study was repeated across the UK, Ireland, Germany, North America and Australia annually. The results were not changing, there was no decrease in the information being found across all countries.

In 2019, the hard drives were sourced from online traders on online platforms such as eBay, Gumtree, Done Deal and the like from within Ireland.

VMGroup used commercial forensic software to conduct the analysis of the hard drives, however it must be pointed out that the information could be retrieved also using opensource tools readily available on the internet.

The analysis conducted attempted to recover deleted items, identify individuals, identify if any encryption was used, identify if any attempts of deletion was performed, identify organisations, retrieve personal information if available and so forth.

Cyber Crime 2019 – Are we really doing anything about it or pointing blame at others? Contd..

The Results

VMGroup found very little change from the 2004 and subsequent years studies. It was scandalous to see that 15 years on, the results were the same.

More worrying, the calibre of information found from organisations was unimaginable. Large financial and auditing firms hard drives were amongst the results, medical practitioners, local councillors and other businesses. From these drives data recovered included financial and personal information belonging to their clients and individuals. All instances of a GDPR breach.

VMGroup summarised the findings in the table below:

Summary of Results
0% of the drives were encrypted
79% of the drives data was deleted or formatted but was still recoverable
14% of the drives contained information for an organisation to be identified
17% of the drives contained information for an individual to be identified
22% of the drives contained copyright material
15% of the drives contained illicit material
14% of the drives contained financial material

Changes in the Security Posture of Organisations and People

It was apparent from the study that not much has changed since the introduction of GDPR in May 2018. Although individuals are aware about their rights in terms of personal information being stored by third parties, they are still not being vigilant when disposing of their own IT equipment.

Additionally organisations are not using simple security measures, such as encryption on devices. Although security standards and regulations are mature in 2019, it is clear they are not being complied with by organisations.

So what next?

The future of data security and IT security can only get better if organisations and individuals practise accordingly to regulation and security standards. It should become the norm for organisations to deploy proper security controls in their area of work.

Although fines have not been administered by Data Protection Commissioner yet in Ireland, it may not always stay in its current state. Organisations should be aware that the consequence of data breach fines is imminent, and they could be the first to get fined if it occurs.

What about the data VMGroup obtained?

If organisations are worried that VMGroup have purchased their previously owned hard drives on the second hand market and currently have their data, please feel free to contact our office to discuss the next steps.

Where an organisation has not come forward, we will liaise with them directly to return the data to them. If they do not want the data returned, VMGroup will wipe all the data beyond recovery. In any case, if no response is received, the data will be wiped within the next 14 days.

Where an organisation is worried about their own data security, VMGroup team of specialists can provide security advisory and help them improve their security posture.

Last piece of Advice

No matter that size your organisation is, data security and an information security strategy should be high in priority on the risk register. If you are unsure about your security posture, contact one of our team of specialist at www.vmgroup.ie