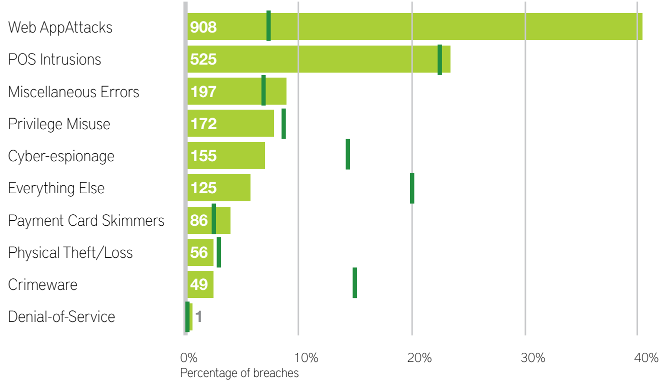
REALDOLMEN
a Gfi Group company

HYBRID CLOUD
IDENTITY SECURITY

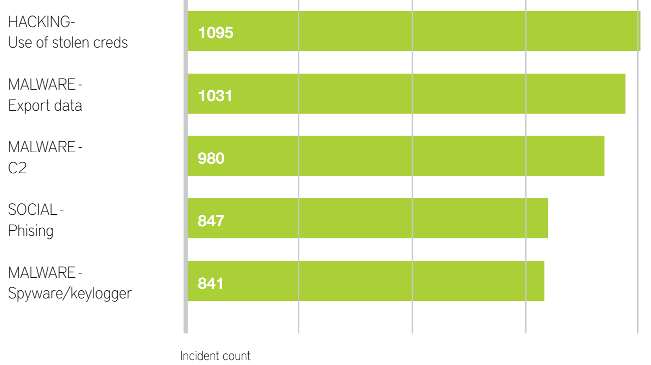
Hybrid Cloud Identity Security

Verizon publishes every year its annual Data Breach Investigations Report (DBIR). Every year again, organizations send their data on thousands of security incidents and data breaches to Verizon, whose researchers analyze that information to highlight new patterns, steady trends and interesting tidbits in the evolving digital threat landscape.

PERCENTAGE, AND COUNT OF BREACHES PER PATTERN.



TOP THREAT ACTION VARIETIES WITHIN INCIDENTS INVOLVING CREDENTIALS



source: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

THE 2016 DBIR QUOTES:

- Incidents in over 82 countries
- In the public, entertainment, finance, and information sectors
- More security incidents than data breaches
- Confirmed disclosure (not just potential exposure) of data to an unauthorized party
- 1,429 incidents of credential theft

Unfortunately often not enough effort is made in mitigating potential security threats. Security should be a concern of everyone in every company, from C-level to System Engineer. However, security precautions that were “hot” some years ago do not apply anymore. A new way of thinking is needed to make sure our company data remains our company data, and nobody else’s.

ASK YOURSELF THIS

Among many others, these are some questions you should ask yourself with your own environment in mind:

DO YOU HAVE LOADS OF OVERPOWERED ACCOUNTS LIKE DOMAIN ADMINS?

Granting superfluous permissions would create abilities beyond the authorized scope of work. We only want to provide users with access permissions they effectively need to perform their day to day tasks.

CAN YOU TRACE BACK ACTIONS TO THE PERSON PERFORMING THEM, THE TIME OF EXECUTION AND THE SOURCE SYSTEM?

Auditing should always be an integral part of any IT organization, making it possible to visualize what went wrong, by whom, when and where.

ARE YOUR WEB APPLICATIONS PUBLISHED SECURELY TOWARDS THE OUTSIDE WORLD?

Making applications accessible to users outside the network is one thing, doing this is in a secure manner is something entirely different.

DO YOU HAVE USER LIFECYCLE MANAGEMENT IN PLACE FOR USERS LEAVING THE ORGANIZATION OR USERS ATTAINING ANOTHER ROLE WITHIN THE COMPANY?

An inactive user account for example can be leveraged to get access to resources without being noticed since it is a valid account.

ARE PASSWORDS THE ONLY MEANS OF SECURING APPLICATIONS?

Multifactor authentication helps guard access to data and applications. However this is an extra step to be performed by end-users, it can be done seamlessly while adding an extra layer of security

ARE YOU PROTECTED AGAINST PASS-THE-HASH ATTACKS? DO YOU HAVE A PROPER PASSWORD POLICY IN PLACE?

Without a proper password policy solution, one cannot be protected from a series of different attacks. Access to 1 machine can mean access to several machines.

DO YOU MONITOR LOGIN BEHAVIOUR WITHIN YOUR ORGANIZATION? WHERE DO PEOPLE LOG IN FROM? HOW MANY ATTEMPTS DID THEY MAKE?

The vast majority of security breaches take place when attackers gain access to an environment by stealing a user's identity. With a set of specific tools, you can monitor and analyze login behaviour with the help of Machine Learning.

WHAT DO WE OFFER?

Realdolmen is your guide on your journey to a more secure Hybrid Identity. Together we will define how we can transform your current environment towards a level of identity security that belongs to today's era.

During a 4 to 8 days assessment we capture your risks and vulnerabilities. We identify recommendations and define the approach to realize your secure Hybrid Identity.

The conclusions of this assessment are delivered in a ½ day presentation and in a report, including recommendations, industry best practices and project definitions.

In addition to this initial assessment, Realdolmen can provide a yearly follow-up to identify progressions that were made, as security is not a static topic, but an ever evolving journey.

BENEFITS OF A SECURED HYBRID IDENTITY

- Publish applications to the outside world without worries
- Give end users more confidence in IT systems and admins
- No more panic when an external audit is performed.
- No more huge amounts of time spent retracing malicious attacks in your organization
- A smiling Chief Security Officer.

INTERESTED ?

Are you willing to reduce your Company's attack surface? You do not wish to end up in the Verizon Data Breaches report? You want us to be your guide in your journey to a more secure Identity infrastructure?

For more information please contact info@realdolmen.com

E.R.: NV RealDolmen SA, A. Vaucampslaan 42, B-1654 Huizingen.