IDENTIFYING A DATA BREACH **USING BIOMETRIC ANALYSIS**

BALABIT
CONTEXTUAL SECURITY INTELLIGENCE

PASSWORDS **ARE DEAD**

"63% OF CONFIRMED DATA BREACHES LEVERAGE A WEAK, DEFAULT, OR STOLEN PASSWORD."
Verizon 2016 Data Breach Investigations Report

Everyone agrees that passwords are bad. Hackers can break most passwords in a matter of hours, while really good passwords are hard to remember. And even good passwords can be acquired easily using social engineering.

PRIVILEGED USERS REPRESENT **RISK**

Any stolen user credential can be very dangerous to a company – but since privileged users have unrestricted access rights, their credentials are of the highest value, and highest risk. Over the years, the IT Security industry has introduced a number of controls that mitigate risks associated with privileged accounts:

1. Passwords on rotation
2. Multi-factor authentication
3. Privileged Identity/Password Management
4. Session monitoring

While these tools mitigate the risks around privileged accounts, they still depend on a fundamental base: authentication.

ONE-OFF AUTHENTICATION IS **NOT ENOUGH**

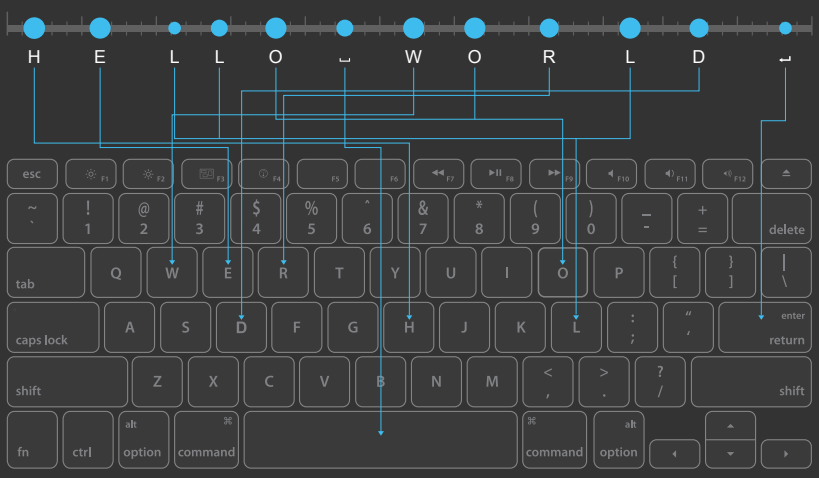
The problem with authentication – be it a simple password or multi-factor authentication – is that it normally happens at the beginning of the session, once. The single measure to tell friend from foe is this one time authentication. Once the authentication is successfully performed, the privileged user is free to do whatever he or she wants until the end of the session, which can be open for several days. If the attacker already has access, none of the existing controls will prevent or detect malicious activities. This is the reason why companies should ensure the authenticity of their users continuously – but without constraining them in their day to day work.

BEHAVIORAL BIOMETRICS IS THE NEW AUTHENTICATION

The solution is to look at user behavior continuously by applying behavior analytics and machine learning to privileged users. Behavioral biometrics collects information about how a user interacts with a device; for example how he or she types or moves the mouse or touchpad. It isn't static information; it is dynamic, which makes it very difficult to steal or imitate.

Blindspotter – which is a component of Balabit's Contextual Security Intelligence™ platform – is the only User Behavior Analytics solution capable of analyzing not only log data, but biometric information pertaining to each user. Although users maybe executing the same task, each has their own idiosyncratic pattern of behavior. The algorithms built into Blindspotter are able to inspect these behavior characteristics due to the perfectly precise and timestamped audit trails provided by another element of Balabit's Contextual Security Intelligence™ platform, Shell Control Box. Shell Control Box is a session monitoring solution that enables companies to execute biometric analysis of users without requiring any additional devices, tools or agents. This analysis is based on the usual activities of employees – there is no intrusion as they go about their work.

HOW DOES KEYSTROKE DYNAMICS ANALYSIS WORK?



Keystroke dynamics analysis looks at the manner and rhythm with which a person types on a keyboard. The most typical values regarding a keystroke are dwell time (the time a key pressed) and flight time (the time between releasing a key up and pressing the next key down). These values are the basis for Balabit's unique keystroke dynamics algorithm, which performs the statistical analysis of the users' key press and release time.

But there are other useful methods to identify patterns regarding the usage of a keyboard as well. Special function keys are used differently by each user. One person might prefer Right Shift, while another uses Left Shift. One uses Backspace more often, while others go for Delete. Which users are keen on use of F-keys?

The time that we need to press a key also varies, usually dependent on the size of our hands. Based on that information, it is possible to create a group of keys, which are also unique to each user.

HOW DOES MOUSE MOVEMENT ANALYSIS WORK?

The basic principle of mouse movement analysis is not the position of the mouse cursor, but the relative extent of position as it changes. The most obvious factor is the speed of mouse movement. The idle time between a mouse movement and a click is as typical as the elapsed time between two clicks of a double click. What's more, the angular velocity (the rate of change of angular position of a rotating body – i.e. the mouse cursor) can be also a good characteristic.

Although most of us do not use a computer for painting, figuratively we are continuously drawing spans with the cursor, while we are using the mouse. There are differences not only in the straightness or curvature of our drawn lines, but in the smoothness of these movements as well. Some users move the cursor in one continuous line, while others break it to smaller fragments. Also, fast movements produce curves with different characteristics from slower movements.

SUMMARY

Behavioral biometrics is one of the most promising areas of IT security. Blindspotter's biometric analysis features are not only able to identify breaches, but work as an additional layer of biometric authentication, enabling security analysts to continuously authenticate whether the user is who he says he is.

Balabit's Contextual Security Intelligence™ platform protects organizations in real-time from threats posed by the misuse of high risk and privileged accounts. Solutions include reliable system and application Log Management with context-enriched data ingestion, Privileged User Monitoring and User Behavior Analytics. Together they can identify unusual user activities and provide deep visibility into potential threats. Working in conjunction with existing control-based strategies Balabit enables a flexible and people-centric approach to improve security without adding additional barriers to business practices.