Die ZEIT, 06/01/2017

Who was that?

Whenever you make a bank transfer via the Internet, you leave unique tracks. Using such biometric footprints, a discreet company identifies millions of users on behalf of banks. The users don't know anything about it.

By Eva Wolfangel

Natia Golan watches the hacker with the utmost calmness. The hacker has taken control of the online account of an unsuspecting British bank client making a transfer. As soon as the client is done, the hacker reaches out from a distance, logs in with the client's data and pretends to act from her computer. The password is correct. Even the amount the hacker is transferring, just over a million pounds, is not uncommon for the above-average wealthy clients of this bank. And yet something is different.

It is the small arcs in which the hacker moves the mouse pointer over the screen. When he moves from one position of the transfer form to the next, in order to enter the sum in one field and the account number in the next field, the pointer stops briefly several times. "He's using the touchpad," recognizes Natia Golan. She does not know where the hacker is. She is watching his movements on a computer in Tel Aviv. And her acumen is helped by software: Small red circles mark the particular movement pattern of the hacker on Golan's screen. For comparison, the typical movements of the client, the victim, are displayed in blue.

"We caught him," Golan triumphs. In fact the hacker was not caught, but he was logged out of the account. "We saved the bank more than a million pounds - and it was so easy!" The enthusiasm is part of the job; Golan is Director of Product Management at Israeli startup Biocatch. Discretion is at least as important for this job; at which bank the betrayed client has her account, she will not reveal. And actually Golan shows such examples only to potential new costumers: other banks that want to dismiss hackers with equal ease. The visit to Tel Aviv had a long lead time, because this is a technique developed for secrecy.

So the client does not know that her account was the target of an attack. And neither does she know that her bank pays a company from Israel to make a profile of her. It says how long her forearm is and how flexible her hand is; whether she has a slight tremor; the breadth of her thumb and the size of the smartphone she uses to visit her bank's website; whether she is skillful in handling the phone with one hand; whether she is left-handed; how strong the muscles of her forearm are and how fast her brain reacts to unexpected challenges. "We calculate all that from the movements and activities," explains Golan. In other words, just by visiting the online banking site, the user has generated the data for the profile she did not suspect. A profile that is very likely to be different from any other person in the world.

The discreet company from Tel Aviv is the pioneer of a new technique and its name symbolizes it: Biocatch is a compound word derived from biometrics (from the Greek bíon and métron, for life and measure) and catch. Anyone who is not who he claims to be should be caught - on the basis of individual characteristics of the body and behavior. On the one hand, this promises the ultimate password. On the other, it raises questions about privacy.

Six hundreds factors have been identified by the Israeli developers, and can be remotely calculated from how a person operates an online banking website. "Twenty to thirty of them define you unequivocally and uniquely," says Avi Turgemann, founder of Biocatch. For the 37-year-old

physicist, the British client is simply a distinctive number; one of 40 million active online banking clients around the world on whom his company keeps an eye as soon as they log into their bank accounts. The slim man with trendy glasses with wide temples and short beard stubbles looks like many young creatives in Tel Aviv. But his idea has made him the boss of a growing company with branches in Boston, London and New York. It is obvious, he says: "The only effective solution against attacks in the internet is if one continuously authenticates the clients."

Authentication today is usually done by passwords. And everyone knows the recurring advice: You should choose secure passwords consisting of numbers, letters and special characters, not of whole words... But all good passwords have one thing in common: users cannot remember them; certainly not a different one for each service. That's why most people use simple passwords for all their logins. Stealing these is the simplest exercise for hackers. "A password might protect your account from your family," says Turgemann,"but not from professional attackers." He sits in the kitchen of the company headquarters with a large cup of coffee in his hand. On the wall there are colorful sayings such as "Eat, relax, play", on the table dozens of muesli dispensers with all sorts of cereals. Turgeman goes ahead into the meeting room, where a note is hanging on the door, just like the ones on the toilet door and the fridge: "Don’t forget to lock your screen." Distrust is in their corporate DNA.

The founder explains that his system is constantly learning: whenever the user is online, it analyzes his movements and interactions. Does he check his account balance first or does he make a bank transfer first? Is his right thumb limited in movement? “After about 20 minutes of learning, we can create a fairly accurate profile,” says Turgeman. Next time, 40 seconds of activity will suffice to distinguish between the account holder and an attacker. The probability of thieves being detected by this method correlates with the number of legitimate users who are mistakenly rejected. The banks must therefore decide individually, Turgeman explains, whether to accept a higher rate of rejected clients at a higher level of security, or to allow their users as much comfort as possible and accept that some thieves will not be discovered. He points to a poster on the wall that depicts the connection in several graphics. He is more of a scientist than a salesman; it seems important to him to explain this very precisel,, along with the fact that the accuracy of his system cannot be expressed in single numbers. Finally, he indicates a point where two lines of a chart meet: "That's a typical combination": 91 percent of all attackers are detected, while 0.5 percent of all legitimate bank clients are mistakenly rejected. "Most banks can live with that".

Behind such percentages is a large number of real people. With the Royal Bank of Scotland, Europe's third-largest bank is one of Biocatch's customers. No other bank has allowed the company to advertise its name. But Turgeman claims that other customers are three of the five largest banks in the UK and the largest in Spain, Italy, Brazil and North America. Not all of them tell the Biocatch boss how many fraud attempts his system is thwarting, but he assumes thousands of cases every week. His algorithms currently monitor two billion transactions per month, says Turgemann, which is around 66 million a day.

The founder of the company had his favorite trick patented. Turgeman speaks cautiously, calmly and deliberately, which makes him seem very modest. But now, when he presents the "invisible challenge", he grins proudly: This trick helps him to make a quick decision in ambiguous situations. To do this, the software will let the mouse pointer disappear briefly or delay the time after which a letter appears on the screen after an input. "The user does not notice that at all, but his brain automatically reacts to it" - and this reaction is highly individual, if measured accurately.

"I know how terrorists and attackers think," says Turgeman. Before becoming a digital entrepreneur, he had hunted hackers for six years in the elite unit 8200 of Israeli intelligence. Turgeman seems to have learnt a lot from the digital espionage force: when he quit his job, he

developed firstly a technology that can filter and intercept conversations from noisy environments, and then an app for mobile payments. When he observed the first fraud attempts, he came up with the idea for Biocatch. "After all I had the knowledge from the secret serviec how to track and identify attackers online."

Unit 8200 in the military intelligence service Aman is the reason why Israel has become a hotspot for cyber security. There are many like Avi Turgeman. For example, Trusteer, an Israeli start-up company with a computer espionage background purchased by IBM in 2013, has developed a system for behavioral authentication ("Trusteer Pinpoint Detect"), which it presented to the public about half a year ago - after Biocatch. Since then, Turgeman feels like the Biblical David, who was not only faster, but also hunted out the first customers of Goliath IBM.

"We have the more disruptive technology," says product manager Golan. IBM Trusteer relies on fewer detection factors and has no "invisible challenges". They continue to explore sophisticated algorithms, says Yaron Wolfsthal, head of the IBM Cyber Security Center of Excellence in the Negev Desert. He looks like the Turgeman counterpart: large, established, self-confident and accuracy is not as important to him as to Turgeman either: How exact the predictions of the IBM system are, he could not say. "We are constantly working to make our system better and better."

Germany lacks not only such a secret service unit, but also a certain carelessness about privacy. Although there are approaches to such research, they still seldom end up in products. A typical example: more than five years ago, scientists at the Ludwig Maximilian University in Munich (LMU) were already working on a smartphone that would use the data from its sensors and entries in all apps to determine whether it was in the hands of a thief, and if so then lock itself. A shrug of the shoulders is all you get today if you ask the people involved what has become of it. Nothing.

Whereby there is no lack of need. "Security is still an unsolved problem, because many users are undermining it," says Florian Alt from LMU. Therefore, the latest trend is to keep people out of the whole thing, as behavioral biometrics does: the user does not actively identify himself, he is identified. "We can observe extremely well what people are doing today," says Alt," right up to the doorknob, which in the future may be able to recognize homeowners by the way they walk towards the house and how hard they press the door handle." The door would then only open for the right person; the key a thing of the past. This is how it should work on the Internet, Alt hopes. His team at LMU is one of the strongest university groups in Germany, and is trying to reconcile usability and security. The Center for Digitization of Bavaria funds the Munich researchers with 1.2 million Euro to explore the opportunities of behavioral biometrics. Alt emphasizes: "Part of the research also consists of determining user acceptance." He even wants them to decide how much privacy they are willing to give up for more comfort.

Avi Turgemann experiences the difference in security cultures during negotiations with a (of course unnamed) German bank: "They are worried because our service is in the cloud" - and not on their own server. But that can be changed." But perhaps these banks are also afraid of the reaction of their clients. Do they want a former intelligence agent to be able to calculate their arm length and cognitive abilities to produce an unmistakable digital fingerprint? Both Avi Turgeman of Biocatch and Nir Stern of Trusteer emphasize that they have no private information about the bank clients; at least not their names. Therefore, they insist, they do not need their consent;it was not about personal data.

"It's misleading to say that's not personal information," says Angela Sasse, professor of Human-Centred Security at University College, London. "From the point of view of computer science, we know that large datasets can remove anonymity." Those who have enough information can draw conclusions about the individual. In addition, a technology that uniquely identifies people on the

Internet without their knowledge and involvement easily arouses desires, warns Sasse. "For targeted advertising, that's an issue." The computer scientist has often observed that companies have set up and trained their systems with seemingly harmless applications in order to offer them to the advertising industry for a lot of money. "Such technologies are introduced through the back door without taking social costs into account." And in the world of post-Snowden, one can easily imagine more delicate applications than penetrating advertising.

Security expert Amir Herzberg of Bar Ilan University in Tel Aviv knows all about the authentication and tracking scene and has worked with all sorts of methods to identify people on the Internet. "We have more than enough problems with privacy issues," he says. Despite all the assertions about the safety of behavioral biometric profiles, he has seen too many vulnerabilities to believe that. And if they were hacked that would be a particularly serious problem. Herzberg warns: "Unlike a password, a normal citizen can hardly change his biometric data."

IBM researcher Yaron Wolfsthal is visibly annoyed by such reservations. "When will we finally stop worrying?" he asks. "Computer security is a cat-and-mouse game: We always have to be one step ahead of the hackers. We benefit more from this technology than it costs us."
However, this can be seen differently. One could also ask: How much is our freedom worth to us? If security costs us personal freedom, it is expensive to buy. But for many, the decision has already been made. Turgeman's algorithms alone monitor two billion transactions per month. During the approximately ten minutes in which you have read this article, BioCatch has observed, evaluated and learned almost half a million processes. Without the clients noticing - and without being asked.