



Security Advisory

Overview: MICROS Systems, Inc. (MICROS) has received a report from one of its customers of an attempt to obtain protected cardholder data using a social engineering attack. The attacker contacted the customer by telephone and represented himself as *MICROS Support*. The attacker requested the customer provide him with credit card data from the MICROS system in order to protect this data from an imminent system failure. This customer suspected foul play and did not provide any information to the attacker. Instead, the customer contacted MICROS customer support and confirmed that MICROS had not been the party making this contact and their MICROS system was not about to fail. It is also important to emphasize that this customer was using a Payment Card Industry Payment Application Data Security Standard (PA-DSS) validated MICROS product, which does not store any unencrypted cardholder data. Therefore, this particular attack could not have succeeded.

Recommendations:

1. MICROS customer support will never contact its customers via telephone or email and request any protected information, such as credit card information or personal information. MICROS strongly recommends that its customers advise their employees and affiliates of this and instruct them never to provide any protected information to anyone calling and claiming to be with MICROS.
2. If you experience this type of attack, please contact MICROS customer support at 1-800-937-2211 and report the incident.
3. All contact between MICROS Customer Support generally relates to a support case with a unique case number. Customers who receive a call from MICROS customer support who wish to verify that this contact is legitimate should request the support case number and the name of the support agent and then should contact the MICROS Support Center at 1-800-937-2211 to verify the contact.