openkey   ARMOR   VENZA. Better Visibility. Better Defense.

Thank you for signing up your team! Good Luck!

2017 HASN'T BEEN EASY

TOP 5 INDUSTRIES BREACHED EACH YEAR

FOOD
RETAIL
HOSPITALITY
FINANCIAL
CYBER SECURITIES

13% INCREASE

DATA BREACHES

164% INCREASE

STOLEN, LOST OR COMPROMISED RECORDS

SECURITY BEST PRACTICES

There are three primary vectors in a hospitality IT environment: **User, Website and Systems.**

#1 USER

- ESTABLISH A THIRD-PARTY USER EDUCATION PROGRAM TO REDUCE MISUSE BY NEGLIGENT AND/OR IGNORANT USERS
- SHUT DOWN THE ABILITY FOR USER TERMINALS TO SHARE RESOURCES PEER-TO-PEER
- IMPLEMENT A DATA BACK-UP STRATEGY FOR PERSONAL DATA ON EXTERNAL DRIVES OR VIRTUAL MACHINES
- INSTALL A REPUTABLE ANTIVIRUS PROGRAM
- CONFIGURE EMAIL PROTECTION MEASURES

#2 WEBSITE

- ENSURE PROPER SEGMENTATION BETWEEN WEB SERVERS AND DATABASE SERVERS
- UTILIZE A DEMILITARIZED ZONE FOR PUBLICLY FACING ASSETS TO PREVENT AN ATTACKER FROM GAINING FURTHER INTERNAL ACCESS SHOULD A BREACH OCCUR
- TRACK VULNERABILITY PATCH STATUS OF CRITICAL DATA SERVERS AND FILE SHARES
- HAVE A BACK-UP STRATEGY FOR DATABASES AND FILE SHARES
- CONSIDER USING SECURE CLOUD OR VIRTUALIZED MACHINES FOR CRITICAL DATA STORAGE AND FILE SHARES OFFSITE

#3 SYSTEMS

- MAINTAIN THE MOST UP-TO-DATE SOFTWARE
- INSTALL A FIREWALL AND ANTIVIRUS SOFTWARE ON BUSINESS SYSTEMS
- CREATE STRONG PASSWORDS FOR BUSINESS SYSTEMS AND CHANGE THEM OFTEN
- MONITOR AND MANAGE ACCESS TO BUSINESS SYSTEMS AND TERMINALS, INCLUDING ELIMINATING REMOTE ACCESS

Resources
1 Breach Level Index 2017 H1 Report
2 2017 Data Breaches – The Worst So Far
3 Best Practices for Lowering Ransomware Risk Armor Blog