INTERACTIVE SESSION: TECHNOLOGY

MWEB BUSINESS: HACKED

BMWEB, launched in 1997, became South Africa's leading ISP in 1998. It has established itself as a company that provides a cutting-edge network and service infrastructure and outstanding customer service. Currently, MWEB's customer base of 320,000 includes home users; small, medium, and large business customers; and corporate clients. MWEB won the ISP of the Year award at the MyBroadband Conference in Johannesburg in 2010. The award was based on the performance of its various broadband services as well as on customer satisfaction.

Its business division, MWEB Business, was founded in January 1998. MWEB Business prides itself as being a business partner that is perfectly positioned to leverage the power of Web-based technologies in all areas of an organization. MWEB Business helps companies:

- Manage business data in ways that add real value and insight to their operations.
- Integrate existing systems with the Internet so as to close the gap between technology, strategy, and the organization's bottom line.
- Develop, manage, and maintain solutions that include all aspects of Internet connectivity, Web site development and hosting, broadband and wireless applications, e-commerce, and consultancy services .
- Manage internal information among employees, as well as among business partners and suppliers.

MWEB has moved forward in publicizing its plans for the South African Internet market. According to MWEB CEO Rudi Jansen, the company needs to improve the quality of their network, which is not only an MWEB problem, but also a Telkom network problem. Despite having a less-than-ideal network infrastructure, MWEB uses AVG Internet Security to offer its customers the best possible security while online. AVG Internet Security offers MWEB customers the following features:

- Identity protection for safe banking and shopping
- LinkScanner for safe surfing and searching
- WebShield for safe social networking, chatting, and downloading
- Antiphishing and antispam for a safe uncluttered inbox
- High-speed antivirus/antispyware software with automatic updates
- An enhanced firewall

In addition, MWEB automatically protects customers against junk email and viruses that are sent via email. Its virus filter ensures that only virus-free email is delivered to clients' inboxes by automatically cleaning e-mails from recognized malware sources. MWEB advises its customers to keep their ADSL connections safe from bandwidth theft and account abuse by blocking unsolicited incoming connections to network ports commonly used by hackers.

Despite the multitude of security services offered by MWEB, a number of MWEB Business subscribers' account details were compromised when their login and password details were published on the Internet by hackers. Initial reports indicated that as many as 2,390 users of MWEB's business digital subscriber lines were affected. The company disclosed the security breach on October 25, 2010. It appears that hackers gained access to Internet Solutions' self-service management system, which MWEB Business uses to provide and manage business accounts that have not yet been migrated to the MWEB network.

Historically, MWEB Business was a reseller of Internet Solutions' Uncapped & Fixed IP ADSL services, which were provisioned and managed by MWEB using a Web-based management interface provided by Internet Solutions. All new Business ADSL services provided after April 2010, as well as the bulk of legacy services already migrated, used MWEB's internal authentication systems, which were completely unaffected by this incident.

MWEB responded quickly to the hacking incident. According to Jansen, about 1,000 clients on the Internet Solutions network needed to be migrated from the old server that was attacked by hackers. Although the network was quickly secured, most customers had recently been moved to MWEB's IPC network. MWEB also contacted these customers to reset their passwords as an added security measure. Jansen was quick to note that no personal information was lost and that none of MWEB's clients suffered any losses as their usernames and passwords had been recreated and changed. He further added that MWEB successfully repels 5,000 attacks a day.

Andre Joubert, general manager of MWEB Business, emphasized that only ADSL authentica-

tion usernames and passwords had been compromised. The integrity of the personal or private data related to the accounts remained intact, as did the access credentials for each customer's bundled onsite router. Joubert did acknowledge the seriousness of the hack, apologizing for any inconvenience the breach may have caused to MWEB's customers. As soon as the breach was identified, MWEB took immediate action to evaluate the extent of the breach and to limit any damage. In MWEB's defense, Jansen said that MWEB constantly advises its customers to be vigilant regarding their online data and security. In addition, MWEB was working closely with Internet Solutions to investigate the nature and source of the breach to ensure that it does not happen again.

Sources: "2010 MyBroadband Awards: The Winners and Losers," MyBroadband, October 19, 2010, http://mybroadband.co.za/news/ broadband/15951-2010-MyBroadband-Awards-The-winners-andlosers. html, accessed November 17, 2010; "About MWEB," MWEB, www.mweb.co.za/productspricing/MWEBBusiness/AboutMWEBB usiness.aspx, accessed November 17, 2010; "Hackers Target MWEB," NewsTime, October 25, 2010, www.newstime.co.za/ ScienceandTech/Hackers_Target_M-Web/13618/, accessed November 17, 2010; "MWEB Business Tackles 'ADSL Hacking' Incident," MyBroadband, October 25, 2010, http://mybroadband.co.za/news/adsl/16077-MWEB-Businesstackles-ADSL-hacking-incident.html, accessed November 17, 2010; "MWEB Business Takes Action in 'Hacking' Incident," Moneyweb, October 25, 2010, www.moneyweb.co.za/mw/view/mw/en/ page295027?oid=5125 45&sn=2009+Detail&pid=287226, accessed November 17, 2010; "MWeb Hacked, Users' Details Exposed," TechCentral, October 26, 2010, www.techcentral.co.za/mwebhacked-users-details-exposed/18366/, accessed November 17, 2010.

Case contributed by Upasana Singh, University of KwaZulu-Natal.

CASE STUDY QUESTIONS

1. What technology issues led to the security breach at MWEB?
2. What is the possible business impact of this security breach for both MWEB and its customers?
3. If you were an MWEB customer, would you consider MWEB's response to the security breach to be acceptable? Why or why not?
4. What should MWEB do in the future to avoid similar incidents?

Early, regular, and thorough testing will contribute significantly to system quality. Many view testing as a way to prove the correctness of work they have done. In fact, we know that all sizable software is riddled with errors, and we must test to uncover these errors.

Good testing begins before a software program is even written by using a *walkthrough*—a review of a specification or design document by a small group of people carefully selected based on the skills needed for the particular objectives being tested. Once developers start writing software programs, coding walkthroughs can also be used to review program code. However, code must be tested by computer runs. When errors are discovered, the source is found and eliminated through a process called *debugging*. You can find out more about the various stages of testing required to put an information system into operation in Chapter 13. Our Learning Tracks also contain descriptions of methodologies for developing software programs that also contribute to software quality.